WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Data Sharing Agreement Implementation Guidance

March 2022, v.2

This guidance was created in collaboration between the Office of Privacy and Data Protection, the Office of Cybersecurity, and the Attorney General's Office as one piece of a privacy and cybersecurity best practices report required by ESSB 5432 (2021). It is intended to help agencies successfully implement appropriate data sharing agreements (DSAs) to protect confidential information.

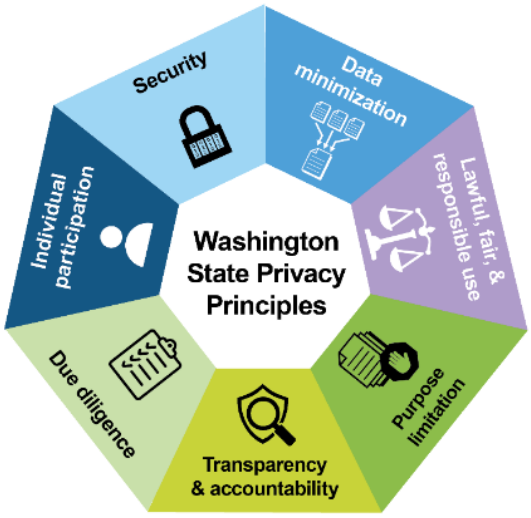
Data sharing relationships take many forms. While this document is a resource that can help agencies assess options, it is not provided for the purpose of giving legal advice of any kind. This guide does not represent the legal opinion of any Washington state agency, including the Attorney General's Office. Readers should not rely on information in this guide regarding specific applications of the laws without seeking legal counsel.

Data Sharing Agreement Requirements

Broad DSA requirements (in addition to requirements that may apply to specific agencies or specific types of information) exist for Washington state agencies in at least three places:

> RCW 39.26.340(1) states that "[b]efore an agency shares with a contractor category 3 or higher data, as defined in policy established in accordance with RCW 43.105.54, a written data-sharing agreement must be place." Within chapter 39.26 RCW, agency means office or activity of the executive or judicial branches of state government.
>
> RCW 39.34.240(1) states that "[i]f a public agency is requesting from another public agency category 3 or higher data . . . the requesting agency shall provide for a written agreement between the agencies . . . ." Within chapter 39.34 RCW, a public agency means any agency, political subdivision, or unit of local government; any state agency; any United States agency; any federally recognized tribe; and any political subdivision of another state.
>
> OCIO Policy #141.10 states that "[w]hen sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law." OCIO Policy #141.10 applies to executive branch agencies and agencies headed by separately elected officials.

Taken individually these requirements could conceivably be interpreted to create a patchwork of DSA mandates. But together they reinforce the best practice that an agency should typically enter DSAs when a person outside the agency receives or has access to confidential information. Entering into DSAs is also consistent with the Washington State Agency Privacy Principles. It is most obviously a core part of the due diligence principle, which requires exercising care when sharing information with third parties. DSAs also support the remaining principles by carrying forward the agency's own obligations as a trusted steward of information and are one part of ensuring an agency understands all the places where its data is located.



Using this Document

This document includes 13 categories of contract terms that should typically be included in a DSA, and seven other terms that might be included depending on the nature of a specific scenario. Each section includes general guidance on implementation, together with example language when possible.

There are core concepts that should typically be included in any agreement that contemplates data sharing, but there is no rigid requirement for a particular format or level of detail. The details of a particular data sharing relationship can significantly impact the overall structure of the agreement, the types of terms to include, the level of detail required and even whether a DSA is feasible at all. For example, when sharing a one-time extract with a researcher, it will be possible to list specific data elements and the specific persons authorized to access the information. When sharing with an IT vendor with broad access to agency data on an ongoing basis, such granularity is not possible.

Based on this variability DSAs may be:

- Standalone or part of a larger agreement.
- One-way or bidirectional.
- Very specific about data elements involved or provide a general description of information.

In determining the appropriate format for a particular relationship, agencies should feel empowered to exercise sound discretion and flexibility. In doing so, they should consider at least:

- The number of parties involved
- Whether sharing is one-way or bidirectional
- The frequency of sharing
- The types of information involved and whether specific legal requirements apply
- The scope of information involved
- The nature of the purpose for sharing
- The nature of the data recipient and the recipient's relationship with the agency

With these considerations in mind, the examples below can be used to create DSAs, or as a tool to review and strengthen existing DSAs. In doing so:

- Do not assume it is just a matter of selecting one option from each section. There may be multiple appropriate terms or none.
- Be ready to add content and narrative. For some terms the content is so situation-specific that templates are not possible.
- Understand that some terms overlap. For example, describing the purpose, appropriate uses, appropriate users, and methods of access do not necessarily need to be five separate contract terms.
- Exercise flexibility only when appropriate for specific terms. A relationship with an IT vendor with broad access to information may warrant flexibility regarding the description of data, but not security requirements.

Should include – Purpose and specific authority for sharing

Describe why the information is being shared and the specific authority for sharing it. Authority to share may come from a variety of places, including laws, contracts, funding requirements, or policies. When sharing with a vendor this may include a description of the agency function being facilitated by sharing the information.

Examples

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

Should include – Description of the data, including classification

Describe the information being shared, including data classification. Include as much specificity as possible, but the level of detail is likely to vary significantly depending on context. For example, listing specific data elements may be appropriate for a one-time arrangement with a researcher, but impracticable for an agreement with a technology vendor that has access to a wide range of information. In some cases, it may be appropriate to execute an overarching agreement with more detailed schedules or attachments executed as needed.

Examples

<table>
<tr><td>Appropriate definitions of protected information</td><td>“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 license numbers, other identifying numbers, and any financial identifiers.

“Confidential Information” or “Data” means information that is exempt from disclosure under chapter 42.56 RCW or other federal or state laws. Confidential Information includes both Category 3 and Category 4 information including, but not limited to, Personal Information.</td></tr>
<tr><td>For broad sharing when data cannot be specifically defined</td><td>Data to be shared includes . . . .

[Describe the data with as much specificity as possible, including at least data classification and the circumstances when information is shared. Where it is not possible to describe specific elements, describing the purpose and processes for sharing provides helpful context].</td></tr>
<tr><td>When listing specific elements is possible</td><td>Data will be exchanged using the mutually agreed upon file layouts below.

i. Method of Access/Transfer: [describe how information is shared]

ii. Frequency of Data Delivery: [describe how often the information is shared]

<table><tr><th>Element Name</th><th>Short Description</th><th>Length</th><th>Type</th><th>Data Descriptions and Usages</th></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table>
[Customize table layout for column names appropriate for the type of data being shared. When sharing multiple extracts with a single recipient, agencies can document this information (and the purpose) for each extract as schedules or addendums]</td></tr>
</table>

Data Classification as its own term	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; ☐ 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, or agreements; b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.
Requirement to specifically notify when Confidential Information is being shared	Agency will notify [Receiving Party] if they are providing Confidential Data.

Should include – Authorized uses

Describe how the information may be used, including prohibited uses. When the agreement is with a contractor performing functions on behalf of an agency, authorized uses should typically be limited to those functions.

Examples

General limitation on permitted uses	This Agreement does not constitute a release of Confidential Information for the Receiving Party's discretionary use and may be accessed and used only to carry out the purposes described in this DSA. Any ad hoc analyses or other use of the data, not specified in this DSA, is not permitted without the prior written agreement of [AGENCY].
General limitation on permitted uses for non-vendors	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 permitted uses of this DSA, 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.
General limitation on permitted uses for vendors	The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except: (1) as provided by law; or, (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.
Prohibition on commercial or personal use	Receiving Party shall not access or use the Confidential Information for any commercial or personal purpose.
Prohibiting data linkage	The Confidential Information shared under this DSA may not be linked with other data sources without prior written agreement of [Agency].
Allowing data linkage	The Confidential Information shared under this DSA may be linked with the following data sources: [*list sources*] [*When allowing data linkage, consider possible impacts such as whether the combined data will be shared with other parties, and whether Agency data will remain identifiable after combination*]
Prohibition on data modifications	The Receiving Party is not authorized to update or change any Data in [Agency system], and any updates or changes will be cause for immediate termination of this DSA.

Should include – Authorized users or classes of users

Describe the specific individuals or classes of individuals who may access the information. This may include subcontractors or other third parties, and any approval process for those subcontractors or third parties.

Examples

Appropriate definitions of Contractor or Receiving Party	"Contractor" means the individual or entity performing services pursuant to this Contract and includes the Contractor's owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents. "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.
General prohibition on sharing with unauthorized users	Receiving Party shall not disclose, in whole or in part, the Data provided by [Agency] to any individual or entity, 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.
General designation of authorized users	Receiving Party must identify: A. Those persons or classes of persons in its workforce who need access to Confidential Information to carry out their duties; and B. For each such person or class of persons, the types of information to which access is needed and any conditions appropriate to such access.
Procedures to limit access	Receiving Party must implement policies and procedures that limit the Confidential Information disclosed to such persons or classes of persons to the amount reasonably necessary to achieve the purpose of the disclosure as described in this DSA.
Subcontractor approval requirements	The Receiving Party will not enter into any Subcontract without the express, written permission of [Agency], which will approve or deny the proposed subcontract in its sole discretion. If Data access is to be provided to a Subcontractor under this DSA it will only be for the specific purpose and uses authorized by [Agency] and the Receiving Party must include all of the Data security terms, conditions and requirements set

	forth in this DSA in any such Subcontract. In no event will the existence of the Subcontract operate to release or reduce the liability of the Receiving Party to [Agency] for any breach in the performance of the Receiving Party's responsibilities. 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).

Should include – Protection of the data in transit if the arrangement involves transmission

If the arrangement involves data transmission, describe how the information will be sent and how it will be protected in transit. If the arrangement involves system access, explain how access will be provisioned.

Examples

Transmission method	*[Describe how the information will be transferred, including applicable encryption protocols or other protections to ensure secure transfer]*
System access	The Receiving Party may request access to [Agency system] for up to [number of] Authorized Users under this DSA. The Receiving Party must send the request for new users to [Agency contact]. Receiving Party must designate a Point of Contact to be the single source of access request for new users. Receiving Party may not use 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). 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. 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 laws governing access to Confidential Information.

Should include – Secure storage for data maintained outside the agency

Describe storage and handling requirements, including applicable encryption at rest or other security requirements.

Examples

General security statement	[Agency] shall take due care and take reasonable precautions to protect Agency's data from unauthorized physical and electronic access. Receiving Party certifies that it complies with the requirements of the OCIO 141.10 policies and standards for data security and access controls to ensure the confidentiality, integrity and availability of all data shared. Receiving party will restrict access to Confidential Information by: A. Allowing access only to staff that have an authorized business requirement to view the Confidential Information. B. Physically securing any computers, documents, or other media containing the Confidential Information. [*This language is not intended to encompass all appropriate security requirements*]

Should include – Data disposal

Describe when and how the information will be destroyed or returned, including a mechanism to verify disposal is completed.

Examples

General disposal requirement	Upon request by [Agency], or at the end of the DSA term, or when no longer needed, Confidential Information/Data must be returned or destroyed using an Agency approved disposal method, except as required to be maintained for compliance or accounting purposes. Receiving Party will provide written certification of disposition using [certificate of disposal, attachment 1]
Disposal of paper records	Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Category 4 information must be destroyed on-site through shredding, pulping, or incineration.

Should include – Backup requirements if applicable

Include backup and recovery specifications when applicable, such as when the recipient is storing the copy of record. Appropriate language will depend on agency needs and the function being performed.

Should include – Incident notification and response

Describe incident response requirements if information is compromised. Include at least requirement to notify, timing, expenses, and roles and responsibilities.

Examples

General notification requirement	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.
Information to be provided	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.
Requirement to mitigate	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].

Notification	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.
Costs	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).
Survival	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.

Should include – Monitoring and enforcement

Describe measures to monitor and enforce the agreement, including remedies for violations. Depending on risk profile and available resources, monitoring could include attestations, verification or audits. At a minimum, remedies should include the right to terminate and have information destroyed or returned.

Examples

General right to monitor and audit	The Receiving Party 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.

Alternative right to audit language	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.
Third party audits	At [Agency's] request or in accordance with OCIO Security Standard No. 141.10, Receiving Party shall obtain third-party 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.
Penalties	Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.

Should include – Awareness and/or training

Describe measures to ensure authorized users understand their responsibilities. Examples could include general privacy training and/or specific nondisclosure agreements for the shared information.

Examples

Employee awareness	The Receiving Party 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] will provide an annual reminder to staff of these requirements. [*Agencies may add to this language to require generic data handling training, or training specific to the agreement*]
Nondisclosure agreements	Individuals will access Data only for the purpose of this Agreement. Each individual shall read and sign [Agency confidentiality and non-disclosure agreement] prior to being granted access to the Data. The Receiving Party will retain a signed copy of [Agency confidentiality and non-disclosure agreement] in each employee's personnel file for a minimum of six years from the date the employee's access to the Data ends. The documentation must be available to [Agency] upon request.

	[*Agencies may modify how long these agreements must be maintained, or proactively collect signed copies prior to sharing information or granting access*]

Should include – Compliance with additional relevant OCIO security requirements based on the type of data sharing

Depending on the specific functions performed by the recipient, compliance with other OCIO security requirements may be required. [Specific security requirements will vary significantly based on the function being performed and agencies are expected to include these requirements as applicable]

Examples

General security statement	The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures in accordance with OCIO security standard 141.10
Alternative general security statement	Receiving Party shall use appropriate safeguards to prevent the inappropriate use, disclosure and/or loss of Confidential Information. Receiving Party shall adopt reasonable and necessary administrative, technical and physical safeguards to ensure the confidentiality, availability and integrity of the Confidential Information. Receiving Party acknowledges that [Agency] is relying on the administrative, physical, and technical safeguards implemented by the Receiving Party in permitting access to Confidential Information subject of this Agreement. The Receiving Party represents and warrants that it has adopted, implemented, and shall maintain, for so long as Receiving Party has access to, creates, maintains, uses, or discloses [Agency's] Confidential Information adequate and appropriate safeguards in order to: (i) protect the confidentiality and security of Confidential Information obtained from, or created on behalf of, [Agency] by the Receiving Party, and (ii) prevent the use or disclosure of Confidential Information other than as provided for by this Agreement and applicable laws. Receiving Party administrative, physical, and technical safeguards and those of its subcontractors, shall comply with all applicable laws, and applicable then current privacy and security guidelines and/or standards issued by the National Institute for Standards and Technology (NIST).

Should include – Any other requirements imposed by law, regulation, contract or policy

Include any other specific data sharing requirements that apply to the information. For example, HIPAA includes specific requirements for contracts with business associates accessing protected health information on behalf of a covered entity.

Might include – Term and termination

Describe the effective term, which may end with a date or an event. Although not unique to data sharing agreements, including an appropriate term provision ties directly into data minimization and purpose limitation. Appropriate termination provisions tie directly into adequate enforcement remedies.

Examples

General term language	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 DSA. The DSA may be extended by mutual agreement through an amendment.
Termination for convenience	Either party may terminate this DSA with [# of days] days' written notice. 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.
Termination for cause	[Agency] may terminate this DSA for default, in whole or in part, by written notice to the Receiving Party, if [Agency] 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. If it is later determined that the Receiving Party was not in default, the termination shall be considered a termination for convenience.

Might include – Off-shore prohibition

Include a prohibition on storing or sharing information outside of the United States when prohibited by law, contract or policy. Even when not formally prohibited, before allowing information to be stored outside of the United States consider the ability to protect the information and seek recourse in a foreign jurisdiction. Also consider the criticality and sensitivity of the information, including the impact of the loss of confidentiality, integrity or availability.

Examples

General prohibition	Receiving Party must maintain all hardcopies containing Confidential Information in the United States. Receiving Party may not directly or indirectly (including through Subcontractors) transport or maintain any Data, hardcopy or electronic, outside the United States unless it has advance written approval from [Agency].

Might include – Cyber liability insurance

Cyber liability insurance is a specific type of insurance coverage to protect an agency from the costs associated with a data breach or other cyber security issues. It is discrete from the commercial general liability requirements often included in agency contracts and the technology errors and omissions insurance that may be appropriate for contracts with IT vendors.

When sharing confidential information with outside vendors, agencies should require sufficient cyber liability coverage to protect the state in the event of a privacy or security incident. The appropriate amount many vary depending on the type and amount of information being shared, and the amount of information from other organizations covered by the policy.

State agencies may have their own cyber liability insurance purchased through the Department of Enterprise Services.

Might include – Indemnification

This term serves to compensate an agency for harm or loss arising in connection with a vendor or contractor's actions or failure to act. The intent is to shift liability away from an agency on to the indemnifying party. Generally, this term should be included in all vendor and contractor agreements. It is typically not appropriate for agreements between two public agencies.

Examples

General indemnification	The Contractor shall be responsible for and shall indemnify, defend, and hold [Agency] harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines, of whatsoever kind of nature, arising out of or relating to a) the Contractor's or any Subcontractor's performance or failure to perform this Contract, or b) the acts or omissions of the Contractor or any Subcontractor. b. The Contractor's duty to indemnify, defend, and hold [Agency] harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines shall include [Agency's] personnel-related costs, reasonable attorney's fees, court costs, and all related expenses. c. The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees. d. Nothing in this term shall be construed as a modification or limitation on the Contractor's obligation to procure insurance in accordance with this Contract or the scope of said insurance.

Might include – Third party requests

Consider including processes for handling requests for information from third parties. This may include court orders and subpoenas or the Public Records Act, particularly when sharing information with other public agencies.

Examples

When sharing with other agencies	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 [Agency] Public Disclosure Officer within five (5) business days and to follow the procedure set out in this section before disclosing any records. The Receiving Party must provide a copy of the records with proposed redactions to [Agency] when they are available and ready. [Agency] will respond within ten (10) business days of receipt of the redacted records to identify concerns with disclosure of the records, propose any changes to the Receiving Party redactions, or request more time if needed. If Receiving Party disagrees with any of [Agency's] concerns or proposed changes, Receiving Party must notify [Agency] of that disagreement and provide [Agency] with a minimum of fifteen (15) business days to obtain a

	restraining order or injunction under RCW 42.56.540 before disclosing any records.
Acknowledgment of Public Records Act for bilateral sharing	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 or information submitted to [Agency] by Receiving Party may also be construed as "public records" and therefore subject to public disclosure.

Might include – Restrictions on disclosure or publication

Some data recipients, such as researchers, may intend to publish data or analysis. Consider including publication procedures, such as de-identification standards or agency review prior to publication.

Examples

General right to review publications	Any and all reports utilizing the data shall be subject to review by [Agency] prior to publication or presentation. [If the recipient will publish analysis or reports using the data, consider the right to review. Also incorporate actual review process, including timelines for review]
Detailed right to review publications	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.
Small numbers requirements	Receiving Party will adhere to [Agency small numbers guidelines] in any published reports. [Agency] and Receiving Party may agree to individual exceptions in writing (email acceptable).

Might include – Other widely applicable contract terms

There are many generic contract terms (i.e. boilerplate) that may be appropriate for a DSA, that are not specific to the data sharing arrangement itself. Examples include governing law, severability, and order of precedence. These types of terms should be included when appropriate, and care should be exercised to ensure consistency when the DSA terms are used as an addendum or exhibit to another contract.

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 [Agency], or created, maintained, or received by you on behalf of [Agency]. 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:		

Version History

Version	Summary of Changes
December 2021 – v.1	N/A
March 2022 – v.2	Clarifies that indemnification clauses are typically not appropriate for agreements between public agencies.