JEFFERSON COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA REQUEST

TO: **Board of County Commissioners**

FROM: **Josh D. Peters, AICP, Community Development Director**
Greg Ballard, Development Code Administrator

DATE: **June 02, 2025**

SUBJECT: **CONSENT AGENDA: Data Sharing Agreement with DAHP for confidential and sensitive archaeological and historic data**

STATEMENT OF ISSUE:

Jefferson County Department of Community Development (DCD) requests Board approval of a Data Sharing Agreement (Agreement) between the Washington State Department of Archaeology and Historic Preservation (DAHP) and Jefferson County.

ANALYSIS:

The purpose of this Agreement is to ensure that shared confidential information is distributed, safeguarded, and utilized solely for its intended purposes. It establishes guidelines for data access, handling, and security measures concerning sensitive cultural resource data. The Agreement specifies authorized users and fosters intergovernmental coordination. Access to the data will be restricted to the individuals listed in Appendices A and B.

This Agreement enables DCD to review archaeological data maintained by DAHP as part of the development permit process. This review supports the protection of archaeological resources and ensures that necessary studies are requested.

The Agreement has been approved as-to-form by the Prosecuting Attorney's Office.

FISCAL IMPACT:

There is no charge for this service. There is no fiscal impact.

RECOMMENDATION:

DCD requests Board approval of the Data Sharing Agreement between DAHP and Jefferson County (Agreement No. 1527).

REVIEWED BY:

Mark McCauley, County Administrator — Date 5/29/25

Clear Form

CONTRACT REVIEW FORM

(INSTRUCTIONS ARE ON THE NEXT PAGE)

CONTRACT WITH: Washington State Department of Archaeology and Historic Preservation Contract No: DCD-DAHP 1527

Contract For: Data Sharing Agreement with DAHP Term: 7 years from date of execution

COUNTY DEPARTMENT:	Community Development
Contact Person:	Chelsea Pronovost
Contact Phone:	(360)379-4494
Contact email:	CPronovost@co.jefferson.wa.us

AMOUNT: N/A

Revenue: _____

Expenditure: _____

Matching Funds Required: _____

Sources(s) of Matching Funds _____

Fund # _____

Munis Org/Obj _____

PROCESS:

- [x] **Exempt from Bid Process**
- [ ] **Cooperative Purchase**
- [ ] **Competitive Sealed Bid**
- [ ] **Small Works Roster**
- [ ] **Vendor List Bid**
- [ ] **RFP or RFQ**
- [ ] **Other:** _____

APPROVAL STEPS:

STEP 1: DEPARTMENT CERTIFIES COMPLIANCE WITH JCC 3.55.080 AND CHAPTER 42.23 RCW.

CERTIFIED: [ ] **N/A:** [■] Signature 5/13/25 Date

STEP 2: DEPARTMENT CERTIFIES THE PERSON PROPOSED FOR CONTRACTING WITH THE COUNTY (CONTRACTOR) HAS NOT BEEN DEBARRED BY ANY FEDERAL, STATE, OR LOCAL AGENCY.

CERTIFIED: [ ] **N/A:** [■] Signature 5/13/25 Date

STEP 3: RISK MANAGEMENT REVIEW (will be added electronically through Laserfiche):

Electronically approved by Risk Management on 5/19/2025.
State agreement - cannot change.

STEP 4: PROSECUTING ATTORNEY REVIEW (will be added electronically through Laserfiche):

Electronically approved as to form by PAO on 5/29/2025.
State contract. Risk management decision. Agreement required to comply with governor's executive order. No mutual hold harmless and county assumes all liability including payment of attorney's fees. Will need to be recorded as an ILA.

STEP 5: DEPARTMENT MAKES REVISIONS & RESUBMITS TO RISK MANAGEMENT AND PROSECUTING ATTORNEY(IF REQUIRED).

STEP 6: CONTRACTOR SIGNS

STEP 7: SUBMIT TO BOCC FOR APPROVAL

Allyson Brooks Ph.D., Director
State Historic Preservation Officer

DATA SHARING AGREEMENT

AGREEMENT No. 1527

Between the

Washington State Department of Archaeology and Historic Preservation

and

Jefferson County

1. Purpose & Sharing Authority

1.1. The purpose of this Data Sharing Agreement (DSA) is to set forth the understanding between the Washington State Department of Archaeology and Historic Preservation (DAHP) and the Jefferson County (Receiving Party) relating to the terms and conditions under which DAHP will allow the restricted use of its confidential and sensitive archaeological and historic data ("Confidential Information" or "Data") by the Receiving Party and the essential measures in which the Confidential Information may be obtained and used within the Receiving Party's digital and physical information technology (IT) systems.

1.2. This DSA ensures that the shared Confidential Information is dispensed, protected, and used only for purposes authorized by this DSA and the State, federal and local statutes governing such use, establishes essential data sharing reciprocity, critical IT security requirements, and applicable cultural resource preservation protocols between the Department and the Receiving Party.

1.3. To support DAHP's statutorily sanctioned functions and the Receiving Party's statutory obligations to evaluate permit applications and other planning activities for their potential impacts on Washington State's non-renewable cultural resources under state, local, and federal law, DAHP is authorized under 10 CFR §800.11(C) to share Confidential Information exempt from disclosure by the Public Records Act (RCW 42.56) and the 1967 Freedom of Information Act (32 CFR § 701.25 - 5 USC 552).

1.4. The Department of Archaeology and Historic Preservation is the State's official central repository for records identifying the location and nature of archaeological and historic sites within the State of Washington and the primary Agency with knowledge and expertise in archaeology and historic preservation. Additionally, DAHP is Washington's advocate for the statewide preservation of irreplaceable historic and cultural resources - significant buildings, structures, sites, objects, and districts - as assets for the future and is the principal Agency responsible for the development of statewide and interagency technical policies, standards, and procedures governing the reporting, collection, and security of cultural resources

information per RCW 27.34, 43.334, 43.105.450, the National Historic Preservation Act of 1966 (36 CFR Part §60), 36 CFR Part §61, 36 CFR §800.16, and 16 USC 470f.

2. Definitions

3.

3.1. "Receiving Party" means the entity identified in Section 1 of this DSA that is a party to this DSA, including the entity's owners, members, officers, directors, partners, trustees, employees, and Contractor(s).

3.2. "Contractor" means the individual or entity performing services pursuant to this DSA and includes the Contractor's owners, members, officers, directors, partners, employees, and agents, unless otherwise stated in this DSA. For purposes of any permitted subcontract, "Contractor" includes any subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

3.3. "Data Downloader" is the Receiving Party's responsible individual for being notified of DSA deliverables and granted specific permission to access to retrieve the Data.

3.4. "WISAARD IT Solution" means the collective information technology (IT) system that DAHP uses to host, encrypt, disseminate, and restrict access to Confidential Information. WISAARD stands for the Washington Information System for Architectural and Archaeological Records Data and is comprised of, but is not limited to, DAHP-procured geographic information system (GIS) technology, software (such as Esri's Enterprise ArcGIS Portal, ArcGIS Server, ArcGIS Datastore, and Microsoft's SQL Server), hardware, connectivity, licenses, and staff resources necessary for system administration.

3.5. "Area of Interest" is where the Receiving Party requests DAHP Confidential Information. This area is within the boundary of Washington State and relates to the Receiving Party's specific jurisdiction.

3.6. "Term" is defined as the length of time between this DSA's Effective Date and seven (7) years unless terminated earlier.

3.7. "Effective Date" is the date on which the DSA becomes effective and is the date when the DSA is signed by the last of the two parties.

3.8. "Encryption" is the process of changing plaintext into a ciphertext for security, integrity, and privacy.

3.9. "At Rest" is data that is not being accessed and is stored on a physical or logical medium. Examples may be files stored on file servers, records in databases, documents on flash drives, hard disks, etc.

3.10. "In Transit" is data that travels through an email, web, or collaborative work applications such as Microsoft Teams or any other type of private or public communication channel.

3.11. "Data Security Classification" is the security protocol established by the Washington State Office of Chief Information Officer (OCIO) under Policy 141.10 through their applicable statute authority to set statewide information technology (IT) policies, standards, and processes under RCW 43.105.450. These OCIO Data Security Classifications are:

3.11.1.1. OCIO Data Category 4 means information explicitly protected from disclosure by state or federal law that requires special handling, such as data associated with the

Health Insurance Portability and Accountability Act (HIPPA), Personally Identifiable Information (PII) safeguarded under the Privacy Act Nonpublic Personal Information (NPI) protected under the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, etc. This information includes but is not limited to a name (i.e., full name, maiden name, mother's maiden name, or alias), personal identification numbers: social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number.

3.11.1.1.1. "Nonpublic Personal Information (NPI)" 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, home addresses, telephone numbers, social security numbers, driver license numbers, other identifying numbers, and any financial identifiers

3.11.1.2. OCIO Data Category 3 is "Confidential Information" specifically protected from disclosure by state or federal statute. Category 3 Data means cultural resources information that is exempt from disclosure under Chapter 42.56 RCW or other federal or state laws, such as the location and associated information of archaeological sites, districts, burials, human remains finds, traditional cultural properties, archaeological cultural resource reports, historic archaeological information, and archaeological resources listed on the National Register of Historic Places and the Washington Heritage Register Listed Resources. Confidential Information for purposes of this DSA is comprised of Category 3 data and records.

3.11.1.3. OCIO Data Category 2 is "Sensitive Information," which is not protected from disclosure by law but is for official use only. Sensitive Information is generally not released to the public unless explicitly requested.

3.11.1.4. OCIO Data Category 1 is "Public Information, " which can be or is currently released to the public without a DSA. This information does not need protection from unauthorized disclosure but does need integrity and available protection controls. DSA covered information that is Category 1, such as the Historic Property Inventories (HPI), National Register of Historic Places, and the Washington Heritage Register-listed historic structures (Register) are designated Public Information under this agreement and do not require any special attention prior to release to the public.

4. Description of DSA Shared Information and OCIO Data Security Classifications

4.1. DAHP shall disseminate annually to the Receiving Party, OCIO Category 1, 2, and 3 information for a defined Area of Interest within the State of Washington so long as there are DAHP staffing and software resources to support DAHP's Data Sharing Program.

4.2. DAHP shall provide the DSA-covered information to the Receiving Party, does not include third-party data (e.g., base maps, census data, soil type, parcels, etc.), and only contains the information listed and classified within Table 1. This information represents Washington State's cultural resource geographic information system (GIS) layers, associated Washington State Plane South Zone NAD 83 HARN projection files, supporting documentation,

accompanying attribute data (stored within Microsoft Access databases), and Federal Geographic Data Committee (FGDC) compliant metadata.

4.3. As may be requested by the Receiving Party, DAHP will provide limited information regarding the appropriate qualifications for cultural resource specialists (i.e., archaeologist, historian, architectural historian, etc.) to facilitate the organization's cultural resource preservation work.

Table 1

DAHP Shared Confidential Information & OCIO Data Security Classification

Information Name	OCIO Category	Required Receiving Party Action
Register Archaeology	3	*Protect – Not for Disclosure*
Register Public	1	*Public – Disclosable*
Archaeology Sites	3	*Protect – Not for Disclosure*
Archaeology Districts	3	*Protect – Not for Disclosure*
Cemeteries & Burials	3	*Protect – Not for Disclosure*
Archaeology Survey Reports	3	*Protect – Not for Disclosure*
Historic Structure Survey Reports	1	*Public – Disclosable*
Historic Properties Inventories	1	*Public – Disclosable*
Maritime Sites	2	*Protect – Disclose if Specifically Requested*
Statewide Archaeological Predictive Model	1	*Public – Disclosable*
Technical briefs, brochures, bulletins, and any other materials addressing preservation planning issues, as may be requested.	1	*Public – Disclosable*
Tribal Consultation Areas (*Areas of Interest Provided to DAHP by the Tribes*)	1	*Public – Disclosable*
Qualification Information for Cultural Resource Specialists	1	*Public – Disclosable*

4.4. The Receiving Party acknowledges that DAHP is subject to the Public Records Act (Chapter 42.56 RCW), that this DSA is a public record, and that any documents or information submitted to DAHP by the Receiving Party may also be construed as a public record and therefore may be subject to public disclosure.

4.5. The Receiving Party shall share information with the Department of Archaeology and Historic Preservation through this DSA that will be maintained by DAHP in accordance with state and federal public records statutes and conform to Agency policies and procedures. Such information may include, but is not limited to:

4.5.1. Publicly available contact information for DSA participants solicited through this DSA will be kept confidential by DAHP unless specifically requested per RCW 42.56;

4.5.2. The Receiving Party's Area of Interest in a GIS shapefile where DAHP Confidential Information is requested, the accompanying Washington State Plane South Zone NAD 83 HARN projection files (.prj), and Federal Geographic Data Committee (FDGC) compliant metadata;

4.5.3. Copies of written reports and inventory forms prepared by the Receiving Party's staff members, contractors, or other professional archaeologists;

4.5.4. Any data, maps, models, and surveys generated by its GIS systems regarding archaeological sites and historic resources;

4.5.5. If available, a GIS parcel layer with parcel numbers and landowner names assists DAHP in mapping historic and archaeological;

4.5.6. A GIS layer of cemetery districts, if available;

4.5.7. Generated technical briefs, brochures, bulletins, and any other materials addressing preservation planning issues, as may be requested or available;

4.5.8. Project-related communication and parameters necessary for DAHP to provide the Receiving Agency responses to consultation requests under the applicable statutes;

Table 2

Receiving Party Shared Data & OCIO Data Security Classification

Information Name	OCIO Data Category	Required DAHP Action
Limited DSA Participant Contact Information	2	*Protect – Disclose if Specifically Requested*
Area of Interest, Project Files, and Metadata	1	*Public – Disclosable*
Generated Archaeological Site Inventories	3	*Protect – Not for Disclosure*
Generated Archaeological District Inventories	3	*Protect – Not for Disclosure*
Generated Cemeteries & Burial Inventories	3	*Protect – Not for Disclosure*
Generated Historic Structure Cultural Resource Survey Reports	1	*Public – Disclosable*
Generated Archaeological, Traditional Cultural Property, & Cemetery Cultural Resource Survey Reports	3	*Protect – Not for Disclosure*
Generated Historic Properties Inventories	1	*Public – Disclosable*
Generated Maritime Site Inventories	2	*Protect – Disclose if Specifically Requested*
Generated Models	1	*Public – Disclosable*
GIS Parcel Layer w/ Owner Information	2	*Protect – Disclose if Specifically Requested*
GIS Cemetery Districts	3	
Generated Technical briefs, brochures, bulletins, and any other materials addressing preservation planning issues, as may be requested.	1	*Public – Disclosable*
Project Consultation Documentation	1	*Public – Disclosable*

5. Response to Development Activity

5.1. The Receiving Party shall promote the preservation of archaeological, historic, and cultural resources protected under state and federal statutes (https://dahp.wa.gov/project-review/preservation-laws), seek to mitigate unavoidable negative impacts to cultural resources, and discourage demolition of historically significant structures.

5.2. The Receiving Party will follow a procedure that will result in an analysis of proposed project impacts and require mitigation of potential effects when (as is appropriate) a development activity is subject to, but not limited to, the State Environmental Policy Act (SEPA), Shoreline Management Act (SMA), Growth Management (GMA), Governor's Executive Order 21-02, or other applicable local ordinance and is proposed within a known archaeological or historic site (or is within an area of high likelihood for the presence of unrecorded sites).

5.2.1. The Receiving Party shall require the project proponent to initiate an Archaeological Excavation Permit with DAHP when proposed ground disturbance activity is unavoidable and within an archaeological or historic site.

5.2.2. The Receiving Party shall consult with DAHP in writing (preferably over email) and concerned tribes to solicit their comments on the proposed measures to avoid, protect, or mitigate effects on the archaeological site.

5.2.3. The Receiving Party shall negotiate consultation procedures between each tribe and the Receiving Party and, where applicable, ensure that consultation requirements of the Governor's Executive Order 21-02 are met.

5.2.4. The Receiving Party shall stipulate that the project proponents engage a Secretary of the Interior professionally qualified archaeologist (per 36 CFR Part 61, Appendix A) to investigate potential impacts to associated cultural resources, provide mitigation recommendations, generate documentation in line with the Washington State Standards for Cultural Resource Reporting, and deliver all relevant reports and material to DAHP and the Receiving Party.

5.2.5. The Receiving Party shall condition project approvals based on DAHP recommendations, the information in the archaeologist's written report, or the conditions outlined within the associated Archaeological Excavation Permit to avoid impacts and promote the conservation of protected cultural resources.

6. Awareness and Training

6.1. The Receiving Party shall assign a staff member responsible for historic preservation program efforts, compliance with this DSA, and ensure said staff attends annual DAHP-sponsored or other cultural resource training(s), if available.

6.2. The Receiving Party shall ensure that all users, administrators, and new personnel with access to the Data are made aware of its use constraints, limitations, disclosure restrictions, and security protocols as described in this DSA.

6.3. The Receiving Party shall hold training for all staff with access to the DAHP Data at least once a year, or as appropriate, to inform them of state and federal laws regarding the protection of historic and archaeological resources and the information technology security requirements delineated within this DSA for the handling of said Confidential Information.

7. Use Constraints and Limitations

7.1. DAHP and the Receiving Party recognize that other parties perform the site survey work, and as a result, the accuracy and reliability of the Data may vary. The information is collected from various sources and will change over time without notice. The Receiving Party is also aware that the Tribes do not always share all cultural resource information with DAHP, which inadvertently may show false negatives in DAHP Confidential Information datasets, particularly regarding traditional use properties and sacred sites.

7.2. As such, the Receiving Party understands that the Confidential Information provided under this DSA is on an "AS IS," "AS AVAILABLE," and "WITH ALL FAULTS" basis. Neither the DAHP nor any of its officials and employees makes any warranty of any kind for this information, express or implied, including but not limited to any warranties of merchantability or fitness for a particular purpose, nor shall the distribution of this information constitute any warranty. DAHP and its officials and employees assume no responsibility or legal liability for the accuracy, completeness, reliability, timeliness, or usefulness of any of the information provided: nor do they represent that the use of any of the information will not infringe privately owned rights. The information is not intended to constitute advice or be used as a substitute for specific advice from a professional. The Receiving Party understands that they should only act (or refrain from acting) based upon the supplied Confidential Information

after independently verifying the information and, as necessary, obtaining professional advice regarding your particular facts and circumstances.

7.3. The Receiving Party also acknowledges that the use of DAHP Confidential Data is limited to design, planning, development, and operations functions and does not preclude the need for field surveys for cultural resources in areas where:

7.3.1. Such surveys have not been conducted in the recent past (i.e., within the last five (5) to seven (7) years.

7.3.2. Previous surveys do not meet current professional standards per the Washington State Standards for Cultural Resource Reporting.

7.3.3. Data indicates the need for additional surveys.

7.4. In the amount reasonably necessary, the Receiving Party shall implement policies and procedures that restrict access and limit the disclosure of Confidential Information to achieve the purpose as described in this DSA.

7.5. Receiving Party shall not reproduce, sell, give, bargain, exchange, donate, loan, lease, or otherwise transfer title, possession, allow access, leverage any reproductions of these Data that result in financial gain, or use of any Category 3 Confidential Information received under this DSA by any person, firm, corporation, Contractor, or association without consent from DAHP.

7.6. The Receiving Party shall use extraordinary precautions to ensure no inadvertent disclosures of Category 2 and 3 DSA-covered information and that DAHP is appropriately listed as the authoritative source.

7.7. At no time will the Receiving Party make the DSA-covered Category 2 and 3 Information available to the public via a publicly accessible website, redistribute to a third party, or transmit these Data via email or other electronic methods, unless required by the Public Records Act or court order as these archaeological and associated records and are exempt from public disclosure under RCW 42.56.300.

7.8. The Receiving Party acknowledges that there are no use constraints for DSA-covered Category 1 information.

8. Response to Inquiries

8.1. General inquiries about the existence of Confidential Information locations shall be answered "yes" or "unknown" by the Receiving Party based on the Confidential Information shared through this DSA as RCW 42.56.300 exempts cultural site information from public disclosure.

8.2. The Receiving Party may disclose Confidential Information on an as-needed basis only to the property owner of record and to the Tribal Cultural Resources Manager/Tribal Chairman of Indian Tribes with cultural connections to the area and may refer inquiries directly to DAHP RCW 42.56.300(4).

8.3. The Receiving Party shall respond according to state and federal law to all public disclosure requests and court orders.

8.4. The Receiving Party shall notify DAHP GIS Manager with a copy of the records and proposed redactions before disclosure of any DSA Category 2 (Sensitive Information),

Category 3 (Confidential Information), or their derived work product created with the intention of being published, displayed, or shared with the public.

8.5. DAHP reserves the right to review and may provide comment on such material for usability, sensitivity, accuracy, completeness, DAHP Reporting Standards consistency, and provide the Receiving Party comments or concerns.

8.6. The Receiving Party shall allow a minimum of fifteen (15) business days for DAHP to obtain a restraining order or injunction under RCW 42.56.540 or other legal procedure before disclosing any records containing Category 3 Confidential Information and Category 2 Sensitive Information subject to this DSA or other legal process.

9. Authorized Users

9.1. The Receiving Party shall identify individuals in its workforce who are authorized to access and handle the Confidential Information necessary to carry out their duties to achieve the stated purposes of this DSA within Appendix A and B of this DSA.

9.2. The Appendix A and B listed persons shall read and sign the Confidentiality and Non-Disclosure DSA located in Appendix C before accessing and handling the Confidential Information.

9.3. The Receiving Party shall retain a signed copy of the Confidentiality and Non-Disclosure Agreement (Appendix C) for each Appendix A and B listed individuals within the employee's personnel file (or designated location) for a minimum of six (6) years from the date at which the employee's access to the Data ends and the documentation must be available to DAHP, upon reasonable request.

9.4. The Receiving Party shall require that only the Appendix A Data Downloader and the Appendix B listed Authorized Users are assigned to distinct user accounts for accessing and using internal and external systems that store DSA-covered Data and that these users do not share account credentials.

9.5. This DSA does not constitute a release for the Receiving Party to share the Data with any third parties, including Contractors, even if for authorized use(s) under this DSA, without the third-party release being approved by DAHP and identified in Appendix A or B of this DSA and a signed Non-Disclosure Agreement (Appendix C).

9.6. When a user listed within Appendix A or B is no longer employed or contracted by the Receiving Party, or duties change such that the listed user no longer requires access to the Data, the Receiving Party signatory or current Data Downloader shall notify DAHP in writing as soon as possible, but within no more than five (5) business days wherein DAHP shall update the proper DSA Appendixes.

9.7. The Receiving Party shall specify one (1) person ("Data Downloader") within Appendix A who shall be responsible for, but not limited to:

9.7.1. Acting as the Receiving Party's point of contact for DAHP Data delivery notifications;

9.7.2. Ensuring the Receiving Party IT security protocols conform to this DSA;

9.7.3. Creating and maintaining an active user account in DAHP's WISAARD IT Solution;

9.7.4. Accessing and downloading DAHP Data deliveries to Receiving Party's IT infrastructure;

9.7.5. Integrating DSA Data into the Receiving Party's IT infrastructure and implementing associated internal communication protocols with Appendix B listed users.

9.8. The Receiving Party shall identify and maintain a list of individuals who have a specified need to access or handle DSA Confidential Information within Appendix B, such as IT system administrators, archaeologists, scientists, researchers, environmental planners, etc.

9.8.1. In the event the Data must be provided to a Receiving Party Contractor identified within Appendix B of this DSA, it will only be for the specific purpose and uses authorized by DAHP, and the Receiving Party must include all Data security terms, conditions, and requirements outlined in this DSA in any such subcontract.

9.8.2. In no event will the existence of the subcontract operate to release or reduce the liability of the Receiving Party to DAHP for any breach in the performance of the Receiving Party's responsibilities.

10. Security Requirements

10.1. As archaeological properties are of a sensitive nature, subject to vandalism, exempt from public disclosure consistent with RCW 42.56.300, and the DSA-covered Confidential Information has been identified as Category 3 within the OCIO Data Classification Standard (141.10 (4.1)), the Receiving Party and DAHP agree to adopt institutional protocols and information technology security measures for encryption at-rest and in-transit for all IT solutions that access or contain DSA-covered Data in accordance with the OCIO's Policy 141, Encryption Standards (141.10 (4.3 - 4.4)), and Data Sharing Policy (141.10 (4.2)).

10.1.1. The DSA-covered Confidential Information shall be shared by DAHP to the Receiving Party using the WISAARD IT Solution in compliance with OCIO's Securing Information Technology Assets Policy 141; including but not limited to the OCIO's Policy 141 subsidiary policies and standards and applicable Security Design Reviews conducted by the OCIO's Office of Cyber Security.

10.1.2. The Receiving Party shall use appropriate safeguards to prevent the inappropriate use, disclosure, or loss of Confidential Information. The Receiving Party shall adopt reasonable and necessary administrative, technical, and physical safeguards to ensure the confidentiality, availability, and integrity of the Confidential Information. The Receiving Party acknowledges that DAHP relies on these safeguards implemented by the Receiving Party in permitting access to Confidential Information subject to this DSA.

10.1.3. For so long the Receiving Party has access to, creates, maintains, uses, or discloses DAHP's Confidential Information, the Receiving Party represents and warrants that it shall adopt, implement, and maintain adequate and appropriate safeguards:

10.1.3.1. To protect the confidentiality and security of DSA-covered Data obtained from or created on behalf of DAHP by the Receiving Party;

10.1.3.2. To prevent the use or disclosure of the Data other than as provided by this DSA and applicable laws.

10.1.3.3. To limit access to the DAHP Data to specific users listed within Appendices A and B;

10.1.3.4. To comply with all applicable laws, current privacy and security guidelines, and standards issued by the National Institute for Standards and Technology (NIST) and the State OCIO.

10.2. The Receiving Party agrees that the physical and digital Data assets of archaeological site records and associated information copied from DAHP Data, or generated from new site reviews, shall be kept in a locked, secure location with limited access.

10.3. The Receiving Party shall maintain logs for DSA Confidential Information (both electronic and hardcopy) and record who/what/where/when/how/why the Confidential Information is accessed by Appendix A and B users.

10.4. The Receiving Party must maintain all digital and hardcopy records containing Confidential Information within the United States. The Receiving Party may not directly or indirectly (including through Contractors) transport or keep any Confidential Information (either hardcopy or electronic) outside the United States unless it has advance written approval from DAHP.

11. Monitoring and Enforcement

11.1. The Receiving Party's access to DAHP's enterprise WISAARD IT Solution may be continuously tracked and monitored for compliance with the Terms set out in this DSA.

11.2. DAHP shall have the right, upon reasonable request, to monitor, audit, and review activities and methods in implementing this DSA to assure Receiving Party compliance and to investigate possible violations of this DSA or violations of laws governing access to Confidential Information.

11.3. Upon reasonable notice, the Receiving Party shall allow DAHP to inspect the Confidential Information's provisions for IT security in conformance with this DSA.

11.4. Any disclosure of Data contrary to this DSA is unauthorized, subject to penalties identified in law, and may result in DAHP terminating Data access for Appendix A and B individual(s) and restrictions placed on future agreements with the Receiving Party.

12. Incident Notification and Response

12.1. The Receiving Parting agrees to implement the Confidential Information into its existing cyber security incident response plan(s) and incorporate the following protocols to ensure the security of DAHP Data:

12.1.1. Within one (1) business day of data incident or breach discovery, notify DAHP of compromise (or a potential compromise) of this DSA's Confidential Information that may be a breach which requires notice to affected individuals under RCW 42.56.590, RCW 19.255.010, or any other applicable breach notification law or rule.

12.1.2. Keep DAHP apprised of remediation progress at regular and timely intervals.

12.1.3. If the Receiving Party does not have complete details about the incident, they will report what information is available and seek to provide full details within fifteen (15) business days of discovery.

12.1.4. To the extent possible, initial reports from the Receiving Party to DAHP must include at least the following:

12.1.4.1. 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;

12.1.4.2. A description of the types of information involved;

12.1.4.3. The investigative and remedial actions the Receiving Party or its Contractor took or will take to prevent and mitigate harmful effects and protect against recurrence;

12.1.4.4. Any details necessary to determine 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;

12.1.4.5. Any other information DAHP reasonably requests.

12.1.5. The Receiving Party agrees to take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DAHP.

12.1.6. If notification to individuals, in the sole judgment of DAHP, be made, the Receiving Party shall further cooperate and facilitate notification to required parties, which may include notification to affected individuals, the media, the Attorney General's Office, affected tribe(s), or other authorities based on applicable law;

12.1.7. At DAHP's discretion, the Receiving Party may be required to fulfill notification requirements directly. However, if DAHP elects to perform the notifications, the Receiving Party shall reimburse DAHP for all associated costs.

12.1.8. The Receiving Party shall be responsible for all costs incurred in connection with a security incident, privacy breach, or potential compromise of data, including:

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

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

12.1.8.3. 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), etc.

12.1.9. The Receiving Party further understands that their obligations regarding breach notifications survive the termination of this DSA for any breach or potential breach at any time and continue for as long as the Receiving Party maintains the Data.

13. Term and Termination

13.1. This DSA begins on the Effective Date and will continue for seven (7) years unless terminated earlier in a written agreement signed by the parties (the "Term").

13.2. This DSA may be extended by mutual agreement by a written amendment signed by the parties.

13.3. Either party may terminate this DSA with ten (10) days' written notice.

13.4. The Data protection, confidentiality, use, and disposition requirements of this DSA shall survive termination for as long as either party is in possession of Confidential Information.

13.5. DAHP may terminate this DSA for default, in whole or in part, by written notice to the Receiving Party if DAHP has a reasonable basis to believe that the Receiving Party has:

13.5.1. Failed to perform under any provision of this DSA;

13.5.2. Violated any law, regulation, rule, or ordinance applicable to this DSA;

13.5.3. Otherwise breached any provision or condition of this DSA.

13.6. If it is later determined that the Receiving Party was not in default, the termination shall be considered a termination for convenience.

13.7. In the event either party becomes aware that the Receiving Party has inadvertently or otherwise unintentionally failed to comply with a mandatory condition of this DSA, such party shall provide prompt written notice to the other wherein the parties thereafter shall cooperate to cure any such failure.

13.7.1. If the Receiving Party thereafter fails to cure a material failure to comply with a mandatory condition of this DSA, DAHP may declare this DSA to be in default.

13.8. In the event this DSA is terminated (and to the extent allowed under applicable records retention or other laws), the Receiving Party shall return to DAHP its physical copies of Confidential Information and shall certify (through the "Disposal Certification of DSA Confidential Information" supplied in Appendix D) that all digital and physical DSA covered Data has been permanently deleted from all Receiving Party IT systems (i.e., procured software solutions, virtual/physical servers, other storage systems).

14. Indemnification

14.1. The Receiving Party and its Contractors shall be responsible for and shall indemnify, defend, and hold DAHP 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:

14.1.1. The Receiving Party's or any Contractors' performance or failure to perform this DSA;

14.1.2. The acts or omissions of the Receiving Party or any Contractor.

14.2. The Receiving Party's duty to indemnify, defend, and hold DAHP harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines shall include DAHP's personnel-related costs, reasonable attorney's fees, court costs, and all related expenses.

14.3. The Receiving Party waives its immunity under Title 51 RCW to the extent required to indemnify, defend, and hold the State and its agencies, officials, agents, or employees harmless.

14.4. Nothing in this DSA shall be construed as a modification or limitation on the Receiving Party's obligation to procure insurance in accordance with this DSA or the scope of said insurance.

IN WITNESS WHEREOF, the parties hereto have executed this DSA as of the last date written below:

For the Department of Archaeology & Historic Preservation

By: Morgan McLemore, GIS Manager

(360) 972-4007

Morgan.McLemore@dahp.wa.gov

Date

For Jefferson County

By: Heidi Eisenhour, Chair
Board of County Commissioners

(360) 385-9100

heisenhour@co.jefferson.wa.us

Date

Approved as to form only:

for 05/29/2025

Philip C. Hunsucker Date

Chief Civil Deputy Prosecuting Attorney

APPENDIX A

DATA SHARING AGREEMENT
DATA DOWNLOADER

The Jefferson County has identified the following person as their Data Downloader to perform the tasks and responsibilities outlined within the Data Sharing Agreement (DSA) listed above.

Downloader Name	Kevin Hitchcock
Title	GIS Administrator
Department/Unit	Central Services
Email	kmhitchcock@co.jefferson.wa.us
Phone Number	(360) 385-9365
Address	1820 Jefferson St, Port Townsend, WA 98368

Downloader Name	Michael Perin
Title	GIS Analyst
Department/Unit	Central Services
Email	mperin@co.jefferson.wa.us
Phone Number	(360) 385-9148
Address	1820 Jefferson St, Port Townsend, WA 98368

APPENDIX B

DATA SHARING AGREEMENT
AUTHORIZED USER LIST

Per the parameters specified within the Data Sharing Agreement (DSA) listed above, the Jefferson County has identified the following person(s) as authorized users of DAHP Confidential Information.

Name	Title	Phone	Email
Josh Peters	Community Development Director	(360)385-4450	jpeters@co.jefferson.w.us
Greg Ballard	Development Code Administrator	(360)385-4450	gballard@co.jefferson.wa.us
Mo-chi Lindblad	Principal Planner	(360)385-4450	mlindblad@co.jefferson.wa.us
David Wayne Johnson	Associate Planner	(360)385-4450	djohnson@co.jefferson.wa.us
Donna Frostholm	Associate Planner	(360)385-4450	dfrostholm@co.jefferson.wa.us
Joel Peterson	Associate Planner	(360)385-4450	jpeterson@co.jefferson.wa.us
Andrew Gosnell	Associate Planner	(360)385-4450	agosnell@co.jefferson.wa.us
George Terry	Associate Planner	(360)385-4450	gterry@co.jefferson.wa.us
Lila Stanfield	Assistant Planner	(360)385-4450	lstanfield@co.jefferson.wa.us
Emily Calkins	Planning Technician	(360)385-4450	ecalkins@co.jefferson.wa.us
Nicki Akins	Code Compliance Coordinator	(360)385-4450	natkins@co.jefferson.wa.us
Michael Byers	Community Development Tech	(360)385-4450	mbyers@co.jefferson.wa.us
Kevin Hitchcock	GIS Coordinator / Administrator	(360)385-9365	kmhitchcock@co.jefferson.wa.us
Michael Perin	GIS Analyst	(360)385-9148	mperin@co.jefferson.wa.us
Monte Reinders	Public Works Director / County Engineer	(360)385-9160	mreinders@co.jefferson.wa.us
Eric Kuzma	Asst. Public Works Director / Engineering Services Manager	(360)385-9160	ekuzma@co.jefferson.wa.us

APPENDIX C

CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT

Between the

Washington State Department of Archaeology and Historic Preservation

and

REPRESENTING

Name of Authorized User	**Name of Receiving Party**

I hereby acknowledge that I am accessing/reviewing/copying/administering Confidential Information exempt from public disclosure per RCW 42.56.300. As an Authorized User, I am responsible for following the details outlined within the Data Sharing Agreement (DSA) identified above.

NOTICE – *The Confidential Information (as defined within the DSA listed above) generated by the Department of Archaeology and Historic Preservation (DAHP) is provided on an "AS IS, "AS AVAILABLE," "WITH ALL FAULTS" basis, is collected from various sources, and will change over time without notice. The Confidential Information is not intended to constitute advice or be used as a substitute for specific advice from a professional. Action or inaction based upon the DSA Confidential Information without independently verifying the information and, as necessary, obtaining professional advice regarding the project's particular facts and circumstances. Neither DAHP nor any of its officials, employees, or agents:*

1.) Make any warranty of any kind for the DSA-covered Confidential Information, express or implied, including but not limited to any warranties of merchantability or fitness for a particular purpose, nor shall its distribution constitute any warranty.

2.) Assume no responsibility or legal liability for the accuracy, completeness, reliability, timeliness, or usefulness of any information provided, nor do they represent that its use will not infringe privately owned rights.

I hereby acknowledge that I will comply with this DSA under penalty of perjury.

Authorized User Signature	**Date**

APPENDIX D

DISPOSAL CERTIFICATION OF DSA CONFIDENTIAL INFORMATION

Between the

Washington State Department of Archaeology and Historic Preservation

and

Jefferson County

In accordance with the Data Sharing Agreement (DSA) listed above and on behalf of the Receiving Party, I hereby certify that all physical and digital DSA-covered Confidential Information has been securely destroyed. There are no remnant versions of said Data within my organization's procured physical or digital information technology solutions (i.e., servers, storage devices, infrastructure as a solution, software as a solution, endpoint devices, paper repositories, etc.).

Description of Confidential Information	
Destruction/Return Date	
Method(s) of Disposal/Return	

DSA Confidential Information Disposed of by:

Signature **Date**

Printed Name **Title**