**Contract ID#:**

**Contract Type: Data Sharing Agreement**

**WWU Responsible Department: Campus Wide Contracts Contract Administration**

This Data Sharing Agreement (“DSA”) is made and entered into by and between **WESTERN WASHINGTON UNIVERSITY**, hereinafter referred to as “Western,” and **T2 SYSTEMS,**  hereinafter referred to as “Recipient.” This DSA is an addendum to Western Agreement CMM No:

**1. PURPOSE OF THE AGREEMENT**

The purpose of this DSA is:

Click or tap here to enter text.

**2. DEFINITIONS**

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

“Data Backup” refers to the duplication or archiving of **data** for the purpose of being able to restore them in case of **data** loss.

“Data Category” refers to the 1 thru 4 classifications of the WWU data based on its sensitivity and confidentiality. Each category determines the type of data that is being shared with the Recipient and the proper handling of that data.

“Data Encryption” refers to the process of converting data into secret code to make it unreadable except by the intended recipient(s). Encryption usually employs symmetric and/or asymmetric algorithms. Data encryption can be required during data transmission or data storage depending on the level of protection required for this data.

“Data Storage” refers to the state data is in when at rest. Data shall be stored on secured environments.

“Data Transmission” refers to the methods and technologies to be used to move a copy of WWU Data between systems, networks, and/or workstations.

“Disclosure” refers to the act of making WWU Data known to an individual or entity and may only be done under the conditions of this agreement.

“FERPA” means Federal Family Educational Rights and Privacy Act.

“GLBA” means Federal Gramm-Leach-Bliley Act.

“HIPAA” means Federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191

“Personally identifiable information” or "PII" means any information identified as protected under applicable federal or state law, which may include, but is not limited to, protections provided under FERPA, HIPAA, GLBA, RCWs, or WACs. Examples include information about an individual’s health, finances, education, use or receipt of governmental services, date of birth, addresses, telephone numbers, social security numbers, driver’s license numbers, identification cards, credit card numbers, biometric identifiers, security credentials (e.g., encryption keys and login credentials), and any other identifying information that is protected by law and may lead to substantial harm of an individual.

“RCW” means the Revised Code of Washington.

“Security Design Review” means the process by which the University Information Security Office (ISO) reviews the security measures in a system design to ensure it meets all applicable University, state, federal, and contractual security requirements. Design reviews may have embedded Risk Assessments.

“WAC” means Washington State Administrative Code.

“WWU Agreement” means the underlying agreement to which this DSA is an addendum.

“WWU Data” means data provided by Western, whether that data originated in Western or in another entity. Such data may include personally identifiable information.

**3. PERIOD OF AGREEMENT**

This DSA shall begin on Click or tap here to enter text. or date of execution, whichever is later, and end onClick or tap here to enter text., unless terminated sooner or extended as provided herein.

**4. DATA TO BE SHARED**

The following WWU Data (list and be specific) will be shared with the Recipient under the terms of this DSA:

|  |  |  |  |
| --- | --- | --- | --- |
| Data Field | Description | Purpose1 | How Stored2 |
|  |  |  |  |

Recipient and Western Program Managers will coordinate the addition or removal of WWU Data that is being shared as soon as practicable, with the DSA being revised accordingly.

1. Why the data needs to be shared.
2. Where the data is being stored (e.g., database, file share) and any security controls placed on the data (e.g., encryption, role-based access control, masking)

**5. AUTHORITY**

The signatories to this DSA represent that they have the authority to enter into and bind their respective organizations to this DSA.

**6. DATA CATEGORY**

The highest Category of the WWU Data shared is:

[ ]  Category 1: Public Information

[ ]  Category 2: Sensitive Information

[ ]  Category 3: Confidential Information

[ ]  Category 4: Confidential Information Requiring Special Handling

If more than one data Category of data applies, describe how the WWU Data is stored in the system and whether data of different categories is mixed, or if the confidential data is segregated and has additional security controls. Note that data of mixed categories stored together must be handled using controls required by the highest category: Click or tap here to enter text.

*See* [*Data Classification at Western*](https://security.wwu.edu/data-classification-procedure)

Click or tap here to enter text.

**7. USERS WITH Authorized ACCESS**

The Recipient’s users (individuals or classes of users) with authorized access of WWU data provided under this DSA are:

Click or tap here to enter text.

Access to WWU Data may only be shared with the authorized users listed above. The Recipient will ensure that all authorized users are familiar with and comply with the terms of this DSA.

Recipient and Western Program Managers will coordinate the addition or removal of authorized users and their access to WWU Data prior to the authorized user’s addition or removal, with the DSA being revised accordingly.

**8. Permitted Use of Data**

The Recipient will use and access WWU Data provided under this DSA only for the limited purposes of carrying out activities pursuant to this DSA as described herein, which are:

Click or tap here to enter text.

**9. Non-disclosure of data**

The Recipient shall not disclose or redisclose, in whole or in part, the WWU Data provided by Western to any individual or entity, unless this DSA specifically authorizes the disclosure. WWU Data may be disclosed only to users with authorized access that have the need to use the WWU Data to achieve the stated purposes of this DSA. In the event of a public or otherwise disclosure request for WWU Data, Recipient will notify Western prior to its release.

Recipient shall not access or use the WWU Data for any commercial or personal purpose, other than the stated purpose under this DSA. This also includes, but is not limited to, analysis or derivative data products, or anonymized and aggregated information, based on the WWU Data. Any exceptions to these limitations must be approved in writing by Western.

The Recipient shall ensure that all its authorized users with access to the WWU Data described in this DSA are aware of the use and disclosure requirements of this agreement and will advise new authorized users of the provisions of this DSA.

**10. Protection of Data**

The Recipient will take due care to protect WWU Data from unauthorized physical and electronic access as described in this DSA; and Recipient shall ensure that it is in compliance with all applicable federal and state privacy rules and laws, Washington State Security Standards (OCIO 141 series), [University security and privacy policies](https://policy.wwu.edu/Subject/Information-Technology) and standards, and applicable benchmark privacy and security standards the Recipient has adopted.

1. The Recipient will comply with all applicable laws, rules, and regulations concerning the privacy and security of the WWU Data, including PII, to be shared hereunder, in its creation, collection, receipt, access, use, storage, disposal, disclosure, and processing. Cite applicable federal or state regulations (check all applicable boxes):

[x]  RCW 19.255.010 and RCW 42.56.590 - Personal information—Notice of security breaches

[x]  WAC 516-26-080 - Release of personally identifiable information or education records—Exceptions to consent requirement

[x]  WAC 516-26-085 - Release of information in emergencies

[x]  FERPA

[x]  HIPAA

[x]  GLBA

[x]  Other:Click or tap here to enter text.

1. Cite Recipients benchmark privacy and security standards and/or frameworks it has adopted:

Click or tap here to enter text.

1. Describe where data will be stored at **T2 SYSTEMS,** and the encryption at rest methods.

Click or tap here to enter text.

1. Describe how data will be transferred between Western and **T2 SYSTEMS, .**Please include transfer protocols and encryption methods.

Click or tap here to enter text.

1. All vendors must attest to their security controls in a Security Design Review template Western Washington University provides to {Contracted Entity} and enforce these controls over the life of the contract. The University uses the Higher Ed Community Vendor Assessment Toolkit (known as the HECVAT) as their security design review template. Indicate the individual who shared the Security Design Review with Western’s Information Security Office (informationsecurity@wwu.edu) and the date it was shared.

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

**T2 SYSTEMS, Date**Employee Name, Title: Click or tap here to enter text.

Click or tap here to enter text.

1. The following additional data handling requirements are required:

Click or tap here to enter text.

The Recipient’s completed and signed HECVAT (Higher Ed Community Vendor Assessment Toolkit) and/or VPAT (Voluntary Product Accessibility Template) assessments are incorporated herein by reference.

**11. Data Backup requirements**

Backups must be treated with the same standard of care as production data and are subject to the same requirements as in the Protection of Data section. Additionally, all data backups must be protected with encryption and the encryption keys protected by strong authentication (2-factor or better).

**12. DATA RETENTION SCHEDULE**

Data will be subject to the following retention schedule(s):

Click or tap here to enter text.

**13. DISPOSITION OF DATA**

Upon termination of this DSA, the Recipient shall ensure that all WWU Data as described herein, is removed and destroyed in a secure manner. WWU Data received under this DSA will be removed from computer equipment after it has been used for its stated purposes by using a utility for securely overwriting the data or physically destroying the media in such a way that data cannot be recovered. The Recipientshall certify in writing within ten business days of termination of this DSA that all copies of WWU Data stored on Recipient servers, backup servers, backup media, or other media including paper copies have been permanently erased or destroyed.

**14. REVIEW COMPLIANCE**

The Recipient agrees that Western will have the right, at any time, to monitor, audit, and review activities and methods in implementing this DSA in order to assure compliance therewith, within the limits of Recipient’s technical capabilities.

* **15. Security Breaches**The Recipient acknowledges the legal obligations set out in the following federal and state regulation(s):

**{Choose from below and remove those that do not apply. You may need to add other regulations}**

* RCW 19.255.010 and RCW 42.56.590 - Personal information—Notice of security breaches
* WAC 516-26-080 - Release of personally identifiable information or education records—Exceptions to consent requirement
* WAC 516-26-085 - Release of information in emergencies
* FERPA
* HIPAA
* GLBA
* **Other:** Click or tap here to enter text.
* In the event either party determines that there has been an unauthorized or improper disclosure of WWU Data, including PII, exchanged under this DSA, such party must promptly notify the other party, unless legally prohibited from doing so or specifically directed by law enforcement not to do so, within twenty-four (24) hours (or any shorter period as may be required by Law) after such party becomes aware of it. Such notification will include the nature of the incident, the other party's information that was compromised, and the action taken or to be taken. Additionally, each party will reasonably assist the other party in remediating and mitigating any potential damage. Subject to the Indemnification provisions, each party shall bear the costs of such remediation or mitigation to the extent the breach or security incident was caused by its acts or omissions.
*
* **16. INSURANCE**In addition to the insurance obligations under the WWU Agreement, the Recipient will procure and maintain for the duration of this DSA a Cyber and Privacy Liability insurance policy against all Western and third-party claims or lawsuits which may arise from or in connection with WWU Data provided to the Recipient hereunder; with limits not less than ,000,000 per occurrence or claim, ,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Recipient in this DSA and shall include, but not be limited to, claims involving invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations. For any claims related to this DSA, the Recipient’s insurance coverage shall be the primary insurance coverage. The Recipient hereby grants to Western a waiver of any right to subrogation which any insurer of the Recipient may acquire against Western by virtue of the payment of any loss under such insurance. The Recipient shall furnish Western Contract Administration, Western Washington University, Administrative Services Building, PO Box 29390, 333 32nd Street, Room 142, Bellingham, Washington 98228-1390 with original certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause.
* **17. GENERAL TERMS AND CONDITIONS**

**Amendments** - This DSA may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

**Assignment** - Neither this DSA, nor any claim arising under this DSA, shall be transferred or assigned by the Recipient without prior written consent of Western.

**DSA Management** - The program manager for each of the parties shall be responsible for and shall be the contact person for all communications regarding the performance of this DSA:

 **The Program Manager for Western is:** Please enter name, address, phone and email

**Click or tap here to enter text.**

 **The Program Manager for the Recipient is:** Please enter name, address, phone and email

 **Click or tap here to enter text.**

**Indemnification** – In addition to the other indemnification obligations under the WWU Agreement, the Recipient hereby agrees to defend, indemnify, and hold harmless Western Washington University, its officers, employees, volunteers and agents from all loss, risk of loss, and damages (including fines, expenses, costs, and attorney fees) sustained or incurred by Western or third-parties because of or by reason of any claims, demands, suits, actions, judgments, or executions for damages of any and every kind and by whomever and whenever made or obtained, allegedly caused by, arising out of, or relating in any manner to any use made of WWU Data obtained by the Recipient under this DSA.

Further, in the event that any unauthorized access to or improper disclosure of WWU Data, including PII, is caused by the Recipient’s breach of its security and/or privacy obligations under this DSA, the Recipient shall be responsible for the performance and costs of: (a) a forensic investigation to determine the cause of the breach, if reasonably necessary, after which it shall provide Western with a description of the breach, what WWU Data was affected, and what steps have been taken to mitigate the effects of the breach; (b) providing notification of the security breach as required by applicable law, including any required notification to government and relevant industry self-regulatory agencies; (c) providing credit file or identity monitoring (as required by state law according to the WWU Data, including PII, that was accessed or disclosed); (d) operating an identity theft call center to respond to questions from individuals whose PII may have been accessed or disclosed for a period of at least one year after the date on which such individuals were notified of the unauthorized access or disclosure; and (e) regulatory fines and penalties. However, the Recipient shall have no responsibility to pay costs of remediation that are due to the reckless misconduct, gross negligence, willful misconduct and/or fraud by Western, its officers, employees, volunteers, or agents.

**Termination** - Either party may terminate this DSA with thirty (30) days’ written notice to the other party’s Program Manager named above. In case of termination, any and all WWU Data provided under this DSA shall either be immediately returned to Western or immediately destroyed by the Recipient as described in the DISPOSITION OF DATA section. The Recipient accepts full responsibility and liability for any violations of this DSA by the Recipient or any officer, employee, or agent of the Recipient; and any such violation shall result in immediate termination by Western of this DSA and immediate forfeiture to Western of WWU Data in any form held by the Recipient or any officer, employee, or agent of the Recipient. In such event, the Recipient shall be liable for damages as authorized by law.

**Waiver** - No term or condition of this DSA shall be held to be waived, modified, or deleted, and no breach excused, except by a written instrument signed by the parties hereto. Waiver of any breach of any term or condition of this DSA shall not be deemed a waiver of any prior or subsequent breach.

**Warrantees** - Western makes no warranties as to accuracy of WWU Data and is not responsible for any loss or damage to Recipient resulting from receiving WWU Data under this DSA. By entering into this DSA the Recipient hereby waives any and all claims against Western for any losses or damages arising out of this DSA. Additionally, the Recipient acknowledges that Western is not providing WWU Data under this DSA as a response to a public record request by the Recipient under the Public Records Act.

**18. ALL WRITINGS CONTAINED HEREIN**

This DSA and the WWU Agreement contain all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this DSA shall be deemed to exist or to bind any of the parties hereto.

IN WITNESS WHEREOF, the parties have executed this DSA as an addendum to WWU Agreement CMM ID 16792 .

|  |  |  |
| --- | --- | --- |
| **FOR CONTRACTOR/RECIPIENT:** |  | **FOR Western Washington university:** |
|  |  |  |
| Signature |  | Signature |
| Print Name |  | Print Name |
|  |  |  |
| Title | Date |  | Title | Date |