University of Washington - Data Security and Privacy Agreement

THIS DATA SECURITY AND PRIVACY AGREEMENT (DSPA)

IS HEREBY INCORPORATED INTO AND AMENDS THE ATTACHED CONTRACT BETWEEN THE UNIVERSITY OF WASHINGTON (UNIVERSITY) AND VENDOR, AS OF THE "EFFECTIVE DATE" LISTED BELOW. In consideration of the mutual promises in the Contract and other good and valuable consideration, the parties agree as follows:

I. DEFINITIONS

1. "**University Data**" means all records and information created, received, maintained, or transmitted by the University which is accessed, created, used, stored, copied, or distributed by Vendor, in connection with the Work under the Contract.

2. "**Work**" refers to all services, work, and all activities involved in providing the materials, work product deliverables, or other obligations that are the subject of the Contract.

3. **"Vendor Group"** means, collectively, Vendor and all of Vendor's subcontractors, vendors, suppliers, agents, assignees, and their employees involved in the Work under the Contract.

4. "**Data Breach**" means, for the purposes of this DSPA and Contract, any adverse event where there is harm to University Data, individuals, host(s), or network(s). This includes, but not by way of exclusion, events indicating that University Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this DSPA or the Contract.

5. "**Malicious Code**" refers to malware, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, bot, or other code or mechanism designed to, without consent collect information, gain access, assert control, alter, and/or cause harm to the systems or data of an effected host, network or environment.

II. DECLARATIONS

Parties understand and acknowledge:

1. University retains all ownership, title, rights, and control over all forms of University Data. Any privileges or license granted to Vendor Group under this DSPA or the Contract shall be narrowly construed, to permit only the least amount of access, creation, use, storage, copying, and/or distribution of University Data that is necessary for the Work. University control over University Data specifically includes determining notification requirements in a potential Data Breach.

2. Vendor is in the best position to control the manner and means of how the Work is performed. Therefore, the express intent of the parties is to hold Vendor accountable for information security and privacy standards and practices of Vendor Group, but only as they pertain to the Work.

3. Vendor is already familiar with the compliance requirements of applicable information and security statutes, rules, and regulations related to the Work or University Data. Vendor conducts business consistent with leading principles and practices of information security and privacy.

4. University has a continuing valid interest in obtaining current records and information from Vendor as assurance that Vendor Group is meeting expected standards of performance, and to substantiate Vendor's representations.

III. OPERATIVE PROVISIONS

1. STANDARD OF CARE

    a. Vendor represents and warrants that, with regard to protecting the confidentiality, availability, and integrity of University Data, and safeguarding the privacy rights of individuals identified by University Data, the Work shall be undertaken with all due care, skill and judgment commensurate with good professional practices.

    b. Vendor represents and warrants that the Work shall be undertaken by fully trained and experienced professional personnel capable of efficiently performing work commensurate with the required standard of care.

2. PRIVACY

    a. **General duty to limit collection and use of data.**
    Vendor represents and warrants that in connection with the Work:

        i. All use of University Data by Vendor Group shall be strictly limited to the direct purpose of performing the Work, except to the extent that University has expressly grants permission in writing for such additional uses.
        ii. Collection of data which identifies individuals shall be limited to the minimum required by the Work.
        iii. Where University is subject to duties and restrictions over the permissible use of University Data arising from the rights of third parties, Vendor Group be bound by and shall comply with any and all such duties and restrictions.

iv. If the Work, in whole or part, involves access or delivery of information via a public-facing web site, then Vendor represents and warrants that its current privacy policy is published online, and is accessible from the same web site as any web-hosted application that is a part of the Work. Vendor's privacy policy will provide end-users with a written explanation of the personal information collected about end-users, as well as available opt-in, opt-out, and other end-user privacy control capabilities.

v. If Vendor Group creates technical system log information, aggregated technical usage or traffic data, and/or statistically measured technical usage or traffic data that contains or originated (in whole or part) from University Data, then Vendor Group's use of such data shall be strictly limited to the direct purpose of the Work and Vendor Group's technical security operations and systems maintenance. Vendor Group is prohibited from using such data that personally identifies an individual for secondary commercial purpose (including but not limited to marketing to such individuals, or disclosing data to third parties for reasons unrelated to the primary purpose for originally collecting the data), nor may Vendor Group solicit consent from the identified individual to do so unless the Contract defines a means to do so that does not unduly burden individual privacy rights.

vi. Markings shall be preserved on all University Data indicating copyright, trademark, other proprietary intellectual property interest, reason for confidentiality, or restrictions on distribution.

b. General duty to protect the confidentiality of University Data.
University Data shall be considered confidential by Vendor and Vendor shall have duties, herein defined, and related to the non-disclosure and protection of the confidentiality of such University Data. Vendor represents and warrants that University Data :

i. Shall not be published, copied, or disclosed to other parties, except at the written direction or with the permission of University.

ii. Shall only be duplicated and distributed within Vendor Group to the extent necessary to adequately perform the Work.

iii. Shall be protected by rigorous safeguards (which meet or exceed the required standard of care) against unauthorized disclosure and/or alteration.

c. University Data shall not be considered confidential under the following circumstances: (a) the information is available to the public, but not due to a Data Breach, or fault of the Vendor; or (b) the record and information was independently obtained by Vendor from a third party who is lawfully in possession of such information and not bound by a non-disclosure obligation with respect to such information; or (c) the record and information was already in Vendor's possession for reasons unrelated to the Contract or an existing agreement with University.

3. COMPLIANCE

a. Vendor represents and warrants the Work, the handling of University Data, and the general conduct business with University, shall all be undertaken in full compliance with any and all applicable statutes, regulations, rules, standards and orders of any official body with jurisdiction over Vendor Group or University.

b. Where the Work or University Data is subject to Family Educational Rights and Privacy Act (FERPA) and the use of educational records within the context of the Work is consistent with a "legitimate educational interest", then Vendor acknowledges that it will be designated as a "school official" as defined in FERPA and its implementing regulations.

c. If the Work or University Data is subject to the administrative simplification provision of Health Insurance Portability and Accountability Act and its implementing regulations, including the Standards for Privacy of Individually Identifiable Health Information and the Security Rule (HIPAA), and parties have executed a Business Associate Agreement (BAA), then to the extent that provisions of this DSPA conflicts with HIPAA compliance, the BAA shall supersede this DSPA.

d. Where the Work or University Data is subject to the Export Administration Regulations (EAR), or International Traffic in Arms Regulations (ITAR), Vendor shall provide the University Office of Sponsored Programs such assistance as necessary to ensure compliance.

4. COMPELLED DISCLOSURE

If any member of Vendor Group is served with any subpoena, discovery request, court order, or other legal request or order that calls for disclosure of any University Data, then Vendor shall promptly notify the University unless specifically prohibited by law from doing so. Notification is not prompt if, due to Vendor's delay, University lacks sufficient time to raise objections to the disclosure, obtain a protective order, or otherwise protect University Data by limiting disclosure. Vendor Group shall at Vendor's expense, provide University prompt and full assistance in University's efforts to protect University Data.

5. DATA BREACH RESPONSE

   a. If the nature of the Work involves Vendor Group equipment, software, product(s), host(s), network(s), or environment(s) that may expose University Data to a potential Data Breach, then Vendor shall have an appropriate incident response plan. University may, at its discretion, require Vendor to participate in response planning for Data Breach scenarios and/or “lessons learned” activities following an event that was or might have been a Data Breach.

   b. If Vendor has reason to believe that Data Breach(es) may have occurred on any of Vendor Groups’ equipment, software, products, host(s), network(s), or environment(s), then Vendor shall promptly (and shall not exceed the time periods as may be required by applicable law) alert the University while also taking such immediate actions as may be necessary to preserve relevant evidence, identity the nature of the event, and contain any Data Breach. As soon as becomes practicable, Vendor shall provide the University a written notice describing the Data Breach incident, and provide University further information updates to help University understand the nature and scope of the event. Vendor shall advise University as to what information and assistance is needed from University in order to eliminate the cause, and mitigate the adverse effects of any Data Breach. Vendor shall prioritize devoting sufficient resources as may be required for this effort.

   c. University may direct Vendor to provide notice and credit monitoring, at Vendor’s expense, to the third parties (such as private individuals, entities, and official bodies) determined by University to require notification, or University may do so itself. Unless Vendor is compelled by law to provide notification to third parties in a particular manner, University shall control the time, place, and manner of such notification.

   d. If recovery from the adverse effects of the Data Breach necessitates Vendor’s assistance in the reinstallation of Vendor Group’s technology product(s) (including hardware or software) that are connected with the Work, then Vendor shall cause such assistance in reinstallation to be provided. If Vendor Group is responsible for the Data Breach, then reinstallation assistance shall be at no cost to the University.

   e. If it appears to the University, in its sole discretion, that services or technology provided by the Vendor are a source of the Data Breach, and present an unreasonable risk, then the University may opt to discontinue use of that source of the Data Breach and the University’s corresponding payment obligations under the Contract shall be adjusted equitably.

6. INFORMATION SECURITY ARCHITECTURE

   a. This section III.6 applies to the extent that Vendor Group owns, supports, or is otherwise responsible for host(s), network(s), environment(s), or technology products (including hardware or software) which may contain University Data.

   b. Vendor represents and warrants that the design and architecture of Vendor Group’s systems (including but not limited to applications and infrastructure) shall be informed by the principle of defense-depth; controls at multiple layers designed to protect the confidentiality, integrity and availability of data.

   c. Vendor shall cause Vendor Group to make appropriate personnel vetting/background checks, have appropriate separation of duties, and undertake other such workflow controls over personnel activities as necessary to safeguard University Data.

   d. Vendor shall cause Vendor Group to follow change management procedures designed to keep Vendor Group’s systems current on security patches, and prevent unintended or unauthorized system configuration changes that could expose system vulnerability or lead to a Data Breach.

   e. To the extent that the Work involves software that was developed, in whole or part, by any of Vendor Group, then Vendor represents and warrants that such portion of the Work was developed within a software development life cycle (SDLC) process that includes security and quality assurance roles and control process intended to eliminate existing and potential security vulnerabilities.

   f. Vendor Group shall have appropriate technical perimeter hardening. Vendor Group shall monitor its system and perimeter configurations and network traffic for vulnerabilities, indicators of activities by threat actors, and/or the presence of Malicious Code.

   g. Vendor Group shall have access, authorization, and authentication technology appropriate for protecting University Data from unauthorized access or modification, and capable of accounting for access to University Data. The overall access control model of Vendor Group systems shall follow the principal of least privileges.

   h. Vendor Group shall safeguard University Data with encryption controls over University Data both stored and in transit. Vendor Group shall discontinue use of encryption methods and communication protocols which become obsolete or have become compromised.

i. Vendor Group shall maintain a process for backup and restoration of data. Vendor represents and warrants that within the context of the Work, the appropriate members within Vendor Group are included in and familiar with a business continuity and disaster recovery plan.

j. Vendor Group facilities will have adequate physical protections, commensurate with leading industry practice for similar Work.

k. Vendor shall, at its own expense, conduct an information security and privacy risk assessment, no less than annually, in order to demonstrate, substantiate, and assure that the security and privacy standards and practices of Vendor meet or exceed the requirements set out in this DSPA. Upon written request, Vendor shall furnish University with an executive summary of the findings of the most recent risk assessment.

   i. University reserves the right to conduct or commission additional tests, relevant to the Work, in order to supplement Vendor's assessment. Vendor shall cause Vendor Group to cooperate with such effort.
   ii. If the findings of the risk assessment identifies either: a potentially significant risk exposure to University Data, or other issue indicating that security and privacy standards and practices of Vendor do not meet the requirements set out in this DSPA, then Vendor shall notify University to communicate the issues, nature of the risks, and the corrective active plan (including the nature of the remediation, and the time frame to execute the corrective actions).

7. DSPA RIGHTS AND REMEDIES

All University rights and remedies set out in this DSPA are in addition to, and not instead of, other remedies set out in the Contract, irrespective of whether the Contract specifies a waiver, limitation on damages or liability, or exclusion of remedies. The terms of this DSPA and the resulting obligations and liabilities imposed on Vendor and Vendor Group shall supersede any provision in the Contract purporting to limit Vendor or Vendor Group's liability or disclaim any liability for damages arising out of Vendor or Vendor Group's breach of this DSPA.

8. INFORMATION SECURITY AND PRIVACY INDEMNIFICATION

a. Except as otherwise expressly limited herein or by law, it is the intent of the parties that all indemnity obligations and/or liabilities assumed by Vendor under the terms of the DSPA, be without limit and without regard to the cause or causes thereof including pre-existing conditions, strict liability, or the negligence of any party or parties (including the indemnified party) whether such negligence be *per se*, sole, joint, concurrent, active, or passive; except that Vendor indemnity obligations shall not apply to the extent of liability directly caused by the willful, reckless or malicious acts of University.

b. Vendor further agrees to defend, indemnify and hold University harmless from and against any and all claims, demands, suit, proceedings, judgment, award, damages, costs, expenses, fees, losses, fines of a penal nature, civil penalties, and other liabilities (including the obligation to indemnify others) arising from or connected to:

   i. **Any violation by Vendor Group of such information security and privacy statutes, ordinances, rules, regulations, and orders of any official body with jurisdiction over Vendor Group or University that are applicable under section III.3 of this DSPA**.
   ii. The Work, and/or any and all information or materials provided by the Vendor Group, with respect to any allegation by a third party of **any infringement of any copyright, trademark, patent, trade secret, or other property right**; or **any cause of action predicated on privacy statute, intrusion upon seclusion, public disclosure of private facts, false light, misappropriation of name or likeness, infliction of emotional distress, or other legal theory protecting privacy rights**.
   iii. Any **Data Breach**, in proportion **to the extent of Vendor Group's fault**.

9. INFORMATION SECURITY AND PRIVACY INSURANCE

a. In addition to the types of insurance, and limits of insurance required by Contract, Vendor shall, at its own expense, provide and maintain in force with insurance companies acceptable to University the kinds of insurance and minimum amounts of coverage set forth in subsection "b." Cognizant of the variety of policy forms currently within the insurance industry, the coverages provided under this section may be maintained in one or more types of insurance policies. However, regardless of the types and forms all policies shall:

   i. Name the Board of Regents of the University of Washington as an additional insured and contain an appropriate severability of interests clause. This requirement is waived for professional liability policies.
   ii. Include a waiver of subrogation in favor of University.
   iii. Include cross-liability coverage
   iv. Be primary as to any other insurance or self-insurance programs afforded to or maintained by University.

b. The types of coverages required under the Contract by this DSPA are:

i. **Internet Professional Liability/ Media Liability/ Errors and Omissions Coverage**, with limits of at least $2 million per occurrence / in the aggregate. Relevant policies must include coverages for:

1. Where the nature of Work includes providing a service for a fee: claims arising out of a failure of the insured's **internet professional services** or claims arising out of the rendering or failure **technology services** by insured. Works requiring cover include, without limitations, activities by Vendor's as an internet service provider, application service provider, web portal, web content developer, web site or web-facing application designer, professional services provider that delivers some portion of such services over the internet. Types of claims include, without limitation: any form of improper "deep-linking", plagiarism, misappropriation of intellectual property, and/or unauthorized disclosure of trade secret, confidential, or other protected private or personal information.
2. Where the nature of the Work includes providing or relying upon a product: claims arising from the failure of **insured technology products** (including hardware and software) to perform its intended function or purpose.
3. Where the nature of the Work includes any activities involving access by Vendor to University's hosts or networks, and/or requires Vendor Group to store University Data: claims arising from insured **security / privacy** controls failure including but not limited to: failure of contractor to prevent the transmission of Malicious Code; failure to prevent unauthorized host or network use; failure to prevent unauthorized host or network access; failure to handle, manage, store, destroy, or otherwise control University Data; failure to prevent collection of protected personal information.

ii. **Cyber Liability/ID Theft and Extortion Insurance**, with limits of at least $2 million per occurrence and in the aggregate. Relevant policies must include coverages for:

1. Claims arising from **Cyber Extortion** or any credible threat or series of related threats to attack insured hosts or networks in a specific way.
2. Claims arising from **Crisis management, response costs and public relations expense**.
3. Claims arising from a **Loss of Data** or **Denial of Service** incident effecting insured host(s) or network(s)

iii. Where the potential net aggregate compensation paid or to be paid by University to Vendor over the term of the Contract exceeds $25,000: **Umbrella liability**, with limits of at least $1 million in the aggregate in support of the "Information Security and Privacy Indemnity" obligations voluntarily assumed by Vendor under §III.8 of this DSPA, which after other coverages required of Vendor Group under the Contract or this DSPA, shall be primary to any other insurance of the University, but only for the risks and liabilities assumed under the Contract or this DSPA.

c. Vendor shall include all entities within Vendor Group as insureds under all applicable required insurance policies of Vendor. Alternatively, each entity within Vendor Group may maintain such coverages that comply fully with all insurance requirements stated herein and shall furnish separate certificates of insurance per the requirements herein. Failure of any member of Vendor Group to comply with insurance requirements does not limit Vendor's liability or responsibility.

d. Vendor shall provide the University of Washington Procurement Services Department, at 3917 University Way NE, Seattle, WA 98105-6692, with a certificate of insurance evidencing proof of insurance coverage, within thirty (30) calendar from the Effective Date of the Contract, or prior to commencement of the Work, if requested by University. Vendor shall furnish to University copies of renewal certificates of all required insurance within thirty (30) calendar days after the renewal date. Vendor shall make a best effort to cause certificates of insurance to expressly indicate compliance with each and every insurance requirement specified in this section. If not, Vendor shall provide a statement describing how the certificates satisfy the requirements in this section within thirty (30) calendar days of this Contract's Effective Date. Either insurer(s) or Vendor shall provide University with thirty (30) days prior written notice of either a material change in coverage or termination of policy. Upon request, Vendor shall further provide the University of Washington Procurement Services Department with a copy of the relevant binders or full policy.

e. By requiring insurance herein, University does not represent that coverage and limits will be adequate to protect Vendor. Such coverage and limits shall not limit Vendor Group's liability under the indemnities and reimbursements granted to University in this Contract.

f. If it is determined judicially or by future legislation or rule that the monetary limits of insurance required hereunder or the indemnities assumed under this paragraph exceed the maximum monetary limits or scope permitted under law, it is agreed that said insurance requirements or indemnities shall automatically be amended to conform to the maximum monetary limits or scope permitted under law.

g. In addition to other remedies under the Contract and this DSPA, if Vendor fails to maintain all insurance coverages required by this DSPA, then University may obtain such missing coverage on Vendor's behalf and at Vendor's expense, or University may require that Vendor obtain appropriate coverages as a corrective action plan, per Section III.9 of this DSPA.

10. TERMINATION PROCEDURES

a. Upon expiration or earlier termination of the Contract, Vendor shall ensure that no Data Breach occurs and shall follow the University's instructions as to the preservation, transfer, or destruction of University Data. Vendor shall certify in writing to University that such return or destruction has been completed.

b. If University terminates the Contract due to a material breach by Vendor Group, then Vendor shall, at University's written request, be obligated to continue to provide the Work pending University's reasonable efforts to obtain a substitute Vendor to provide the Work.

11. OPPORTUNITY TO CURE

In the event of a material breach of the DSPA by Vendor Group, the University reserves its rights to terminate the Contract and seek all other available remedies. In lieu of immediately exercising the right to terminate, University may opt to extend to Vendor an opportunity to cure Vendor Group's material breach, and shall contact the Vendor, in writing, to describe issues where corrective action is sought. Within ten (10) business days, Vendor will provide a response, in writing, to explain how Vendor shall address all issues to University's satisfaction. If the Vendor's response is, in whole or part, unacceptable to University, then University may refer the matter to the dispute resolution provision of the Contract, or seek other reasonable means to resolve outstanding issues. To the extent that the Vendor's response describes acceptable corrective actions, then University and Vendor shall coordinate in furtherance of executing Vendor's corrective actions. Vendor shall make a written request to University to confirm that satisfactory performance of corrective actions has cured the material breach. Such acceptance shall not be unreasonably withheld.

12. SURVIVAL; ORDER OF PRECEDENCE

This DSPA shall survive the expiration or earlier termination of the Contract. In the event the provisions of this DSPA conflict with any provision of the Contract, or Vendors' warranties, support contract, or service level agreement, the provisions of this DSPA shall prevail.

IN WITNESS WHEREOF, this Contract has been executed as of the date of the last party to sign below ("Effective Date"). If signed in counterparts, then each shall be considered an original thereof.

UNIVERSITY		**VENDOR**	
X:	_____	**X:**	_____
By:	_____	**By:**	_____
Title:	_____	**Title:**	_____
Date:	_____	**Date:**	_____

University of Washington - Data Security and Privacy Agreement

OPTIONAL EXHIBIT 1 - IDENTIFICATION OF CONTRACT AND CONTACTS

The parties may have optionally provided additional reference information in this section, as a convenience for the administration of the executory contract. Parties agree that this contract is both complete and binding irrespective whether any additional reference information is provided in this exhibit.

ADDITIONAL REFERENCE INFORMATION

Contract identification

Parties have provided the following reference information to facilitate identification of that certain Contract which is hereby amended by this DSPA.

Contract title and/or number: _____

Date of Contract execution: _____

Contract refers to University party of DSPA as: _____

Contract refers to Vendor party of DSPA as: _____

Contact Information

Parties have provided the following contact information to facilitate communication on issues arising from this DSPA:

University Contact name: _____

University Contact Department/Organizational Unit: _____

University Contact telephone: _____

University Contact email: _____

University Contact address: _____

_____

Vendor Contact name: _____

Vendor Contact telephone: _____

Vendor Contact email: _____

Vendor Contact address: _____

OPTIONAL EXHIBIT 2 – INFORMATION SECURITY AND PRIVACY ASSURANCE DOCUMENTATION

The parties may have optionally provided additional reference information in this section, as a convenience for the administration of the executory contract. Parties agree that this contract is both complete and binding irrespective whether any additional documentation information is provided in this exhibit.

Parties have attached the following documentation to this exhibit (check all that apply):

Ref	Document Description	Document Title	Date
§III.3.d	Export control license.		
§III.2.a.iv	Hardcopy of most recently published privacy policy. Please include the URL in the "Document Title"		
§III.6.k	Executive Summary findings from most recent Risk Assessment		
§III.9.d	Proof of insurance coverage		
§III.12	Additional amendments or writings which alter the order of precedence between provisions.		