

DATA SECURITY ADDENDUM

This Data Security Addendum (*Addendum*) is incorporated in and attached to that certain agreement titled _____ and dated _____ (*Contract*) by and between the University of Washington (*University*) and _____ (*Contractor*).

1. Definitions

- a. University Data.** University Data is any and all data within the University’s possession, custody, or control, and any and all data that the University has disclosed to Contractor. For the purposes of this Addendum, University Data does not cease to be University Data solely because it is transferred or transmitted beyond the University’s immediate possession, custody, or control.
- b. Confidential Data.** Confidential Data is University Data that may be: identified with a specific individual (*e.g.*, “personally identifiable information” or “PII”); is subject to proprietary rights under patent, copyright, trademark, or trade secret law; privileged against disclosure in a civil lawsuit (*e.g.*, data subject to the attorney-client or physician-patient privileges); subject to laws, regulations, rules, or standards that prohibit or limit disclosure (*e.g.*, the Family Educational Rights and Privacy Act (FERPA), the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), or the Health Insurance Portability and Accountability Act (HIPAA)); or by the nature of the University Data or the circumstances surrounding its disclosure, ought in good faith to be treated as sensitive, proprietary, or confidential.
- c. Security Breach.** Security Breach means any use, disclosure, loss, or acquisition of, or access to, Confidential Data that is not in accordance with the terms of this Addendum, including Section 3(b) below, or the Contract.
- d. System.** An assembly of components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (network, server, computer, software, application, operating system or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

2. Disclosure of University Data

Contractor shall not use, access, or disclose University Data in any manner—including, without limitation, by means of outsourcing, sharing, retransfer, access, or use—to any person or entity, except:

- a.** Contractor’s employees or agents who actually and legitimately need to access or use University Data in the performance of Contractor’s duties under this Addendum or the Contract;
- b.** Such third parties as may be specifically identified in this Addendum or the Contract, but only after such third party has agreed—in writing and in advance of any disclosure—to be bound by all of the terms of this Addendum; or
- c.** Any other third party approved by the University in writing and in advance of any disclosure, but only to the extent of such approval.

3. Use or Storage of, or Access to, University Data

Contractor shall only use, store, or access University Data:

- a. In accordance with, and only to the extent permissible under, this Addendum and the Contract; and
- b. In full compliance with any and all applicable laws, regulations, rules, or standards, including, to the extent applicable, but without limitation: FERPA, EAR, ITAR, HIPAA, the Gramm-Leach-Bliley Financial Services Modernization Act (GLB), Federal Trade Commission Red Flags Rule, Payment Card Industry Data Security Standards, and RCW 19.255.010 and RCW 42.56.590. Contractor shall notify University in writing if Contractor obtains and export control license for Data covered by EAR or ITAR.

4. Safeguarding University Data

Contractor agrees that use or storage of, and access to University Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Contractor shall implement and maintain all safeguards necessary to ensure the confidentiality, availability, and integrity of all University Data. If any of these safeguards represent a change to a System, these changes shall be implemented by Contractor in accordance with Contractor's approved field modification process at the time of System installation and shall be included in the price of the System.

Such safeguards shall include as appropriate, and without limitation, the following:

- a. **System Security.** A System that is owned or supported by Contractor and contains University Data shall be secured as follows:
 - i. Contractor warrants that their System is free of any system settings or defects that would constitute a potential security risk as defined by University. Contractor shall provide a list of applications, open ports and communication protocols used by their Systems.
 - ii. Contractor's System shall use secure network communications protocols, such as SSH, SCP, HTTPS or IPsec, to safeguard Confidential Data.
 - iii. Contractor understands their System may be placed on a publically routable IP address and warrants the System is sufficiently protected from compromises and attacks. Contractor may need to add a host based firewall or an external firewall to protect the System or Contractor may allow University to add a host based or external firewall without breach of this Agreement, Contractor's warranty or University support contract.
 - iv. Contractor shall coordinate with University to achieve the following:
 - Limit administrative access to the System.
 - Turn off services provided by the operating system that are unnecessary to the proper functioning of the System.
 - Enable disk quotas to ensure System availability.

- Forward System log events to centralized servers.
 - Configure the System to use Kerberos, LDAP or other industry compliant services for authentication and authorization. If the System lacks the capability to utilize centralized authentication and/or authorization infrastructure services, a secure remote API, batch load interface or other mechanism must be provided for provisioning user accounts and privileges to the Systems from a central source maintained by University.
 - Make archival copies of System for backup and recovery or for forensic purposes.
- v. Contractor agrees to review maintenance and security patches for the System made available by the operating system and application software supplier or grant such rights to University. Within a reasonable time frame, Contractor shall review patches and determine if the patches are essential for safeguarding the confidentiality, integrity, or availability of the System or University Data. Contractor shall respond with an analysis and plan of action within five (5) business days of the availability of the critical patches, although verification of loading corrective patches may take longer.
- vi. Contractor System shall allow the changing of System passwords.
- vii. All changes to Contractor System shall be coordinated with and approved in writing by University.

b. System Maintenance and Support

- i. Contractor shall ensure that its System is supported. If the System or any components of the System become unsupported, Contractor shall provide University with a migration plan to a supported System. The migration plan shall be covered by the terms and conditions of Contractor's warranty or University support contract and University shall incur no additional cost.
- ii. Contractor shall provide remote support via a connection that is mutually agreed upon by both parties. The remote support shall achieve the following: transmission of University Data shall be encrypted using a University approved encryption method; remote access should be limited to an as needed or as requested basis by University; creation of all Contractor accounts for remote access must be authorized in writing by University and Contractor shall notify University of separation or reassignment of support personnel; the System must support logging requirements as specified by University. Contractor shall coordinate with University to monitor System activity and configuration, including interactive sessions of Contractor, with prior notice or warning.

c. Data Protections.

- i. Contractor policies and procedures shall prevent any unauthorized use, disclosure loss, or acquisition of, or access to, University Data. This includes, but is not limited to personnel security measures, such as background checks.

- ii. Contractor shall provide University written notice of any director, officer, employee or agent of Contractor that was or is employed by University that has access to or use of University Data. University shall have sole discretion to disallow access to or use of University Data to any person identified in such notice.
- iii. Any and all transmission of University Data to and between Systems shall be performed using a secure transfer method that establishes chain of custody of University Data and is mutually agreed upon by both parties.

5. Oversight

Contractor shall perform a security evaluation, audit, or review on a regular basis to ensure compliance with Contractor's safeguards, any safeguards required under this Addendum or the Contract, and industry best practices for the protection of University Data. Such evaluation, audit, or review shall be performed by independent and credentialed auditors, consultants, or information security professionals. If an evaluation, audit, or review identifies any error, flaw, or inadequacy with respect to any safeguard that does or may affect Confidential Data, Contractor shall promptly notify the University. The University may require that Contractor immediately correct any such error, flaw, or inadequacy, and if Contractor is unable or unwilling to immediately make such correction, the University may immediately terminate the Contract.

6. Security Breach

- a. If Contractor has reason to believe that Confidential Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this Addendum or the Contract, Contractor shall promptly alert the University of any Security Breach, preferably within no more than two business days, and shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the Security Breach. Contractor shall give highest priority to immediately correcting any Security Breach and shall devote such resources as may be required to accomplish that goal. Contractor shall provide the University any and all information necessary to enable the University to fully understand the nature and scope of the Security Breach. To the extent the University, in its sole discretion, deems warranted—whether in accordance with applicable Washington law such as RCW 42.56.590 or RCW 19.255.010, or federal law such as HIPAA, EAR or ITAR—the University may provide notice or require Contractor to provide notice to any or all parties affected by any Security Breach. In such case, Contractor shall consult with the University in a timely fashion regarding appropriate steps required to notify third parties. Contractor shall provide University information about what Contractor has done or plans to do to mitigate any deleterious effect or the unauthorized use or disclosure of, or access to, University Data. In the event that a Security Breach requires Contractor's assistance in reinstalling software, such assistance shall be provided at no cost to the University and in accordance with the University's policies and standards. The University may discontinue any services or products provided by Contractor until the University, in its sole discretion, determines that the cause of the Security Breach has been sufficiently mitigated.
- b. Contractor shall defend, indemnify, and save the University harmless from and against any claims, actions, loss, liability, damage, costs, or expenses, including, but not limited to, reasonable attorneys' fees, arising from any or all Security Breaches. The indemnification provided hereunder includes the full costs of forensics analysis, System remediation to eliminate the cause of the Security Breach, and notice to affected individuals, including, but not limited to, the services of any consulting firm used to counsel the University with regard to providing notice or to actually provide such notice.

7. No Surreptitious Code

Contractor warrants that, to the best of its knowledge, all software or firmware which has been created by Contractor, has been incorporated into Contractor's software or firmware, or may be supplied by Contractor, and which may be used with or in any way affect University Data, is free of and does not contain any self-help code or any unauthorized code as defined below. Contractor further warrants that it will not knowingly introduce, via electronic network connectivity (such as a modem) or otherwise, any code or mechanism that electronically notifies Contractor of any fact or event, or any key, node, lock, time-out, or other function, implemented by any type of means or under any circumstances, which may restrict University's access to or use of University Data.

- a. "Self-help code" means any back door, time bomb, or drop dead device, or software routine, designed to disable a computer program automatically with the passage of time or under the positive control of a person other than a software licensee. Self-help code does not include software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system solely for purposes of maintenance or technical support.
- b. "Unauthorized code" means any virus, Trojan horse, worm, or other software routines or equipment components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data, or to perform any other such actions. Unauthorized code does not include self-help code.
- c. Contractor understands that University may not purchase ongoing support for the System. If license keys are needed for the System to operate, the license key shall be re-activated by Contractor free of charge to University.

8. Compelled Disclosure

If Contractor is served with any subpoena, discovery request, court order, or other legal request or command that calls for disclosure of any University Data, Contractor shall promptly notify the University in writing and provide the University sufficient time to obtain a court order or take any other action the University deems necessary to prevent disclosure or otherwise protect University Data. In such event, Contractor shall provide University prompt and full assistance in University's efforts to protect University Data.

9. Termination Procedures

Upon expiration or earlier termination of the Contract, Contractor shall ensure that no Security Breach occurs and shall follow the University's instructions as to the preservation, transfer, or destruction of University Data. The method of destruction shall prevent any unauthorized use or disclosure of, or access to, University Data.

10. Survival; Order of Precedence

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

UNIVERSITY OF WASHINGTON

[NAME OF CONTRACTOR]

Signature: _____

Signature: _____

Printed Name: _____

Name: _____

Job Title: _____

Job Title: _____