UNIVERSITY OF WASHINGTON – IT SECURITY TERMS

INTRODUCTION, PARTIES, AND EFFECTIVE DATE

THESE IT SECURITY TERMS ARE HEREBY INCORPORATED INTO THE CONTRACT BETWEEN THE UNIVERSITY OF WASHINGTON (UNIVERSITY) AND CONTRACTOR, AS OF THE "EFFECTIVE DATE" OF THE CONTRACT. IN CONSIDERATION OF THE MUTUAL PROMISES IN THE CONTRACT AND OTHER GOOD AND VALUABLE CONSIDERATION, THE PARTIES AGREE AS FOLLOWS:

I. DEFINITIONS

1. "**Incident**" means, for the purposes of this Contract, any adverse event (including technical or physical incidents) 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, unlawfully, or contrary to the terms of the Contract.

2. "**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.

3. "**University Data**" means all records and information created, received, maintained, or transmitted by the University, which are accessed, created, used, stored, copied, or distributed by Contractor, in connection with the Work under the Contract. University Data which meets the criteria for the definition of University Personal Data, as defined within the University Data Processing Agreement (DPA), herein incorporated by reference, should be first interpreted under the DPA, and only interpreted as University Data to the extent that the DPA is not dispositive of the issue.

4. "**Contractor Group**" has the same meaning as "The Contractor" as the term is defined within the University of Washington General Terms and Conditions and additionally includes any person or entity appointed by or on behalf of the Contractor to carry out any portion of the Work.

5. "**Contractor**" has the same meaning as "The Contractor" as the term is defined within the University of Washington General Terms and Conditions.

6. **"Work**" has the same meaning as "Work" as the term is defined within the University of Washington General Terms and Conditions, irrespective of whether the work product includes goods, a license, professional services, or any form of technology solution delivered as a service.

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 Contractor Group under these IT Security Terms, 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 Incident.

2. Contractor 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 Contractor accountable for information security standards and practices of Contractor Group, but only as they pertain to the Work.
3. Contractor is already familiar with the compliance requirements of applicable information and security statutes, rules, and regulations related to the Work or University Data. Contractor conducts business consistent with leading principles and practices of information security.
4. University has a continuing valid interest in obtaining current records and information from Contractor as assurance that Contractor Group is meeting expected standards of performance, and to substantiate Contractor's representations.

III. OPERATIVE PROVISIONS

1. STANDARD OF CARE

   a. Contractor represents and warrants that, with regard to protecting the confidentiality, availability, and integrity of University Data, the Work shall be undertaken with all due care, skill and judgment commensurate with good professional practices.

   b. Contractor represents and warrants that the Work shall be undertaken by personnel capable of performing work commensurate with the required standard of care.

2. UNIVERSITY DATA OWNERSHIP

   a. UNIVERSITY DATA SHALL NOT BE DISCLOSED BY CONTRACTOR GROUP TO A THIRD PARTY, UNLESS THE UNIVERSITY GRANTS PERMISSION IN WRITING TO THE CONTRACTOR TO DISCLOSE, OR UNLESS SUCH DISCLOSURE IS REQUIRED BY APPLICABLE LAW.

   b. MARKINGS ON ALL UNIVERSITY DATA - INDICATING COPYRIGHT, TRADEMARK, OTHER PROPRIETARY INTELLECTUAL PROPERTY INTEREST, REASON FOR CONFIDENTIALITY, OR REASON ON DISTRIBUTION SHALL BE PRESERVED.

3. COMPLIANCE

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

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

4. COMPELLED DISCLOSURE

   a. If the Contractor receives any subpoena, discovery request, court order, or other legal request or order that calls for disclosure of any University Data, then the Contractor shall promptly notify the University unless specifically prohibited by law from doing so. The Contractor's notification shall give the University sufficient time to object to the disclosure,

obtain a protective order, or otherwise protect University Data by limiting disclosure. The Contractor shall provide the University with prompt and full assistance in the University's efforts to protect University Data. Any disclosure pursuant to this section shall be limited to the minimum disclosure required by law.

b. The Contractor shall assist the University by implementing technical and organizational measures, to the extent practicable, in order for the University to meet its obligations (as understood by the University) to respond to requests for production or disclosure of University Data held by the Contractor. The Contractor shall promptly notify the University if the Contractor receives a request for University Data, assist the University in the University's response, and respond to the request for University Data directly only on the documented instructions of the University or as required by applicable laws to which the Contractor is subject, in which case the Contractor shall, to the extent permitted by applicable laws, inform the University of the Contractor's legal obligations before any response to the request for University Data.

5. INCIDENT RESPONSE

If the nature of an Incident involves University Personal Data, as defined in the DPA, then the DPA incident response process shall apply instead of the provisions of these IT Security Terms.

a. If the nature of the Work involves Contractor Group equipment, software, product(s), host(s), network(s), or environment(s) that may expose University Data to a potential Incident, then Contractor shall have an appropriate incident response plan. University may, at its discretion, request Contractor to participate in "lessons learned" activities following an incident.

b. If the Contractor has reason to believe that an Incident has occurred, then, without undue delay, the Contractor shall notify the University of said Incident. Such notification to the University shall include sufficient information to enable the University to meet its obligations under applicable law.

c. In the event of an Incident, the Contractor shall cooperate with the University to:
   i. Investigate and identify the nature of the Incident;
   ii. Preserve relevant evidence;
   iii. Contain, remediate, and mitigate the Incident; and
   iv. Notify the University of any additional or newly emerged information beyond the initial Incident notification to the University described above.

d. In the event of an Incident caused in whole or part by the CONTRACTOR, the University may
   i. instruct the CONTRACTOR, at the CONTRACTOR's expense, to provide notice when required by applicable law, or when an Incident could result in harm to individuals and/or risk to the University;
   ii. and/or Services such as credit monitoring or identity theft protection to individuals when the absence of such services could result in harm to individuals and/or individuals would have a reasonable expectation that such services be provided.
   iii. Alternatively, the University may elect to provide the notice and services itself.

e. If recovery from the adverse effects of the Incident necessitates Contractor's assistance in the reinstallation of Contractor Group's technology product(s) (including hardware or software) that relate to the Work, then Contractor shall cause such assistance in reinstallation to be provided. If Contractor Group is responsible for the Incident, then reinstallation assistance shall be at no cost to the University.

f. If it appears to the University, in its sole discretion, that services or technology provided by the Contractor are a source of the Incident, and present an unreasonable risk, then the University may opt to discontinue use of that source of the Incident 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 Contractor Group owns, supports, or is otherwise responsible for host(s), network(s), environment(s), or the Work involves services wherein Contractor has care, custody, or control of University Data. For avoidance of doubt, this section shall apply when Contractor Group provides cloud-hosted infrastructure, platform, or application as a service.

b. Contractor represents and warrants that the design and architecture of Contractor 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. Contractor shall cause Contractor 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. Contractor shall cause Contractor Group to follow change management procedures designed to keep Contractor Group's systems current on security patches and prevent unintended or unauthorized system configuration changes that could expose system vulnerability or lead to a Incident.

e. To the extent that the Work involves software that was developed, in whole or part, by any of Contractor Group, then Contractor represents and warrants that such portion of the Work was developed within a Software Development Life Cycle process that includes security and quality assurance roles and control process intended to eliminate existing and potential security vulnerabilities.

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

g. Contractor 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 Contractor Group systems shall follow the principal of least privileges.

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

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

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

k. Contractor shall maintain a process for regularly testing, assessing, and evaluating the effectiveness of technical, physical, and administrative measures that meet or exceed the requirements set out under these IT Security Terms and Conditions. Upon request, Contractor shall furnish University with an executive summary of the findings of the most recent assessment.

   i. University reserves the right to conduct or commission additional tests, relevant to the Work, to supplement Contractor's assessment. Contractor shall cause Contractor Group to cooperate with such effort.

   ii. If the findings of an assessment identifies either: a potentially significant risk exposure to University Data, or other issue indicating that security standards and practices of Contractor do not meet the requirements set out under these IT Security Terms and Conditions, then Contractor 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. UNIVERSITY RIGHTS AND REMEDIES

All University rights and remedies set out in these Security terms 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 these IT Security Terms and Conditions and the resulting obligations and liabilities imposed on Contractor and Contractor Group shall supersede any provision in the Contract purporting to limit Contractor or Contractor Group's liability or disclaim any liability for damages arising out of Contractor or Contractor Group's breach of under these IT Security Terms and Conditions.

8. INFORMATION SECURITY INDEMNIFICATION

a. It is the intent of the parties that all indemnity obligations of Contractor with respect to information security be allocated within this section and that any exclusions or limitation of liability language elsewhere within this Contract does not apply to Contractor's information security indemnification obligations.

b. Contractor 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 Contractor Group of such information security statutes, ordinances, rules, regulations, and orders of any official body with jurisdiction over Contractor Group or University that are applicable under the compliance provisions of these Security terms and conditions**.

   ii. The Work, and/or all information or materials provided by the Contractor Group, with respect to any allegation by a third party of **any infringement of any copyright, trademark, patent, trade secret, or other property intellectual property right**.

   iii. Any **Incident**, in proportion **to the extent of Contractor Group's fault**.

9. INFORMATION SECURITY INSURANCE COVERAGE

   Contractor shall, at its own expense, provide and maintain in force the appropriate kinds of insurance and minimum amounts of coverage, sufficient to support Contractor's information security indemnity obligations, as further specified in the attached CYBER LIABILITY RIDER, hereby incorporated by reference.

10. TRANSITION SERVICES

   a. As part of the winding up of services, associated with the expiration or termination of the Contract, the Contractor shall follow the University's instructions as to the preservation, transfer, or destruction of University Data. If, after requesting that University provide instructions, University fails to do so, then the instructions shall be deemed to be that the Contractor shall not destroy and not retain any University Data but shall first transfer to the University any and all University Data in Contractor's possession.

   b. If the Contract terminates due to a material breach or unresolvable dispute, then Contractor shall, at University's written request, be obligated to continue to provide the Work, at Contract rates, pending University's reasonable efforts to obtain a substitute Contractor to provide the Work.

11. OPPORTUNITY TO CURE

   In the event of a material breach of these IT Security Terms and conditions by Contractor 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 Contractor an opportunity to cure Contractor Group's material breach, and shall contact the Contractor, in writing, to describe issues where corrective action is sought. Within ten (10) business days, Contractor will provide a response, in writing, to explain how Contractor shall address all issues to University's satisfaction. If the Contractor'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 Contractor's response

describes acceptable corrective actions, then University and Contractor shall coordinate in furtherance of executing Contractor's corrective actions. Contractor 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

a. With respect to the subject of these provisions, these Security terms and conditions shall supersede the general terms of this contract and shall supersede any terms, within this contract that would otherwise limit the remedies set out herein.

b. If the data processing activity includes University Personal Data, then the DPA governs the data processing. University Personal Data and Data Processing Terms are defined in the DPA.

UNIVERSITY OF WASHINGTON – CYBER LIABILITY RIDER

INTRODUCTION, PARTIES, AND EFFECTIVE DATE

THIS CYBER LIABILITY RIDER IS HEREBY INCORPORATED INTO THE CONTRACT BETWEEN THE UNIVERSITY OF WASHINGTON (UNIVERSITY) AND CONTRACTOR, AS OF THE "EFFECTIVE DATE" OF THE CONTRACT. IN CONSIDERATION OF THE MUTUAL PROMISES IN THE CONTRACT AND OTHER GOOD AND VALUABLE CONSIDERATION, THE PARTIES AGREE AS FOLLOWS:

13. INFORMATION SECURITY INSURANCE COVERAGE

a. In addition to the types of insurance, and limits of insurance required by Contract, Contractor shall, at its own expense, provide and maintain in force the kinds of insurance and minimum amounts of coverage, sufficient to support Contractor's information security indemnity obligations, not less than as 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, irrespective of the name of the type of policy or coverage, such that Contractor is in material compliance with the requirements of this rider.

b. The types of coverages required under the Contract by this Cyber Liability Rider 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 of **technology services** by insured. Works requiring cover include, without limitations, activities by Contractor'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 Contractor to University's hosts or networks, and/or requires Contractor Group to store University Data: claims arising from insured **security** 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, and failure to provide individuals access to information and controls about their personal data as required by law.

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 first- and third-person **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**, including liability arising from failure to notify, legal expenses, and computer forensic expenses.
3. Claims arising from **Unauthorized Access to or use of data,** a **Loss of Data** or **Denial of Service** incident effecting insured host(s) or network(s)

iii. Where the Contract includes IT Special Terms and Conditions and the potential net aggregate compensation paid or to be paid by University to Contractor over the term of the Contract exceeds $25,000: **Umbrella liability**, with limits of at least $1 million in the aggregate, which after other coverages required of Contractor Group under the Contract, shall be primary to any other insurance of the University, but only for the risks and liabilities assumed under the Contract.