CONSTRUCTION SUPPLIER ACCESS AND LICENSE AGREEMENT

THIS AGREEMENT is made between the Arizona Board of Regents, a body corporate, for and on behalf of Arizona State University (ASU) and _____, (Supplier), effective as of _____, 20__ (the Effective Date).

Supplier, as a subcontractor of _____ (Contractor), pursuant to a Standard Form Agreement dated _____, 20__, between ASU and Contractor (CM@RIsk), provided/installed _____ (the Equipment) in ASU's _____ (the Building). The Equipment is owned by ASU, [includes software,] and requires network connectivity and access to ASU's technology and computing network.

In consideration of the mutual obligations in this Agreement, and for other good and valuable consideration, which the parties agree is sufficient, the parties agree as follows:

1. **Access.** Subject to the terms of this Agreement, ASU grants Supplier non-exclusive, non-transferable, limited access to ASU's technology and computing network (ASU's Network), solely to the extent necessary to install, operate, and maintain the Equipment in the Building to the extent described in Exhibit A.

2. **Equipment.** The Equipment is described with specificity in Exhibit A. In connection with the Equipment, CM@RISK will provide services to ASU, and will meet the service level requirements as and when set forth on Exhibit A. Such services and Equipment, together with all reports delivered to ASU pursuant thereto and hereto, are collectively defined as the Deliverables.

3. **[License.** If applicable, add a license from Supplier for any software or ASU access to SAAS]

4. **Technology Security Review.** Prior to installing the Equipment or obtaining access to ASU's Network, Supplier and the Deliverables have undergone, or will undergo, an ASU Technology Security Review. Supplier certifies that all information, data, and documentation provided to ASU as part of the Technology Security Review, when delivered, and during the Term, is, was, and will be true and correct in all material respects.

5. **Information Security.** [All Supplier Deliverables that **include software, services, and devices that store, transmit, or otherwise process,** ASU Data **(each a system)** and/or provide **Supplier** access to ASU's Network] must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable laws, rules, and regulations. ASU Data means: all data and information that ASU provides to Supplier, as well as all data and information managed by Supplier on behalf of ASU, including all output, reports, analyses, and other materials relating to, derived from, or generated pursuant to this Agreement, even if generated by Supplier, as well as all data obtained or extracted through ASU's or Supplier's use of such data or information. ASU Data also includes all data and information provided directly to Supplier by ASU students and employees, and includes personal data, metadata, and user content. To diminish information security threats, **Supplier** will (either directly or through its third party service providers) meet the following requirements:

    a. With respect to each System, CM@RISK and its contractors at all tiers (directly and through their third party service providers) will meet the following requirements:

        1. Access Control. Control access to ASU's resources, including ASU Data, limiting access to legitimate business need based on an individual's job-related assignment, approve and track access to ensure proper usage and accountability, and make such information available to ASU for review, upon ASU's request.

        2. Incident Reporting. Report information security incidents that affect ASU Data immediately to ASU (including those that involve information disclosure incidents, unauthorized disclosure of ASU Data, successful network intrusions, malware infection, and unauthorized access or modifications).

        3. Off Shore. Ensure (i) that all development or modification of software for ASU is performed only within

the borders of the United States, and (ii) all ASU Data (including any backup copies) are stored, accessed from, and otherwise processed only within the borders of the United States. This provision applies to work performed by CM@RISK and their subcontractors at all tiers and to all ASU Data.

4. Patch Management. Carry out updates and patch management for all Systems in a timely manner and to the satisfaction of ASU. Updates and patch management must be deployed using an auditable process that can be reviewed by ASU upon ASU's request.

5. Encryption. Ensure all Systems use an industry standard encryption protocol for sensitive data, personal data, or personally identifiable data, as those terms may be defined in applicable laws, rules and regulations (PII), in transit and at rest (as documented in NIST 800-57, or equivalent).

6. Notifications. Notify ASU immediately if Supplier receives any kind of subpoena for or involving ASU Data, if any third party requests ASU Data, or if Supplier has a change in the location or transmission of ASU Data. All notifications to ASU required in this Information Security paragraph will be sent to ASU Information Security at Infosec@asu.edu, in addition to any other notice addresses in this Agreement.

7. Backup and Restoration. Ensure that all ASU Data is available and accessible, and that adequate systems are in place to restore the availability and accessibility of all ASU Data in a timely manner in the event of a physical or technical threat.

8. Privacy by Design. When developing, designing, selecting, and using Systems for processing sensitive data, personal data, or personally identifiable data, as those terms may be defined in applicable laws, rules and regulations (PII), Supplier will, with due regard to the state of the art, incorporate and implement data privacy best practices.

b. In addition to Section 17(a) above, the following provisions apply if: (i) Supplier receives, stores, or analyzes ASU Data (including if the data is not online); or (ii) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data:

1. Third Party Security Audits. Complete certified third party audit (such as SOC2 Type II or substantially equivalent) in accordance with then current industry standards, which audits are subject to review by ASU upon ASU's request. Currently, no more than two audits per year are required.

2. Penetration Tests. Perform periodic third party scans, including penetration tests, for unauthorized applications, services, code, and system vulnerabilities on each System in accordance with industry standards and ASU standards (as documented in NIST 800-115 or equivalent), and Supplier must provide proof of testing to ASU upon ASU's request.

3. Vulnerability Scanning. All web-based Systems are required to have a remediation plan and third party web application security scans in accordance with then current industry best practices or when required by applicable industry regulations or standards. Supplier must correct weaknesses within a reasonable period of time, consistent with applicable industry regulations or standards, and consistent with the criticality of the risk, and Supplier must provide proof of testing to ASU upon ASU's request.

c. In addition to Sections 17(a)-(b) above, the following provision applies if: (i) ASU is purchasing or leasing software, or processing a software renewal; (ii) Supplier is creating any code for ASU; or (iii) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data:

1. ASU Rights. Allow ASU (directly or through third party service providers) to scan and/or penetration test any System regardless of where it resides.

d. In addition to Sections 17(a)-(c) above, the following provision applies if: (i) ASU is purchasing or leasing software, or processing a software renewal; (ii) Supplier is creating any code for ASU; (iii) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data; or (iv), Supplier is collecting PII or ASU Data via a link on an ASU.edu or other ASU managed webpage:

1. Secure Development. Use secure development and coding standards including secure change management procedures in accordance with industry standards. Prior to releasing new software versions, Supplier will perform quality assurance testing and penetration testing and/or scanning. Supplier will provide to ASU for review, upon ASU request, evidence of a secure software development life cycle (SDLC).

6. **Supplier's Intellectual Property**. Supplier will retain ownership of its pre-existing Intellectual Property, including any that may be incorporated into the Contract IP, provided that Supplier informs ASU in writing before incorporating any pre-existing Intellectual Property into any Contract IP. Supplier hereby grants to ASU a perpetual, irrevocable, royalty- free, worldwide right and license (with the right to sublicense), to freely use, make, have made, reproduce, disseminate, display, perform, and create derivative works based on such pre-existing Intellectual Property as may be incorporated into the Contract IP or otherwise provided to ASU in the course of performing under the Agreement.

7. **Data Use, Ownership, and Privacy**. The terms of this section apply if Supplier receives, has access to, stores, or analyzes any ASU Data (as defined above). As between the parties, ASU will own, or retain all of its rights in, all data and information that ASU provides to Supplier, as well as all data and information managed by Supplier on behalf of ASU, including all output, reports, analyses, and other materials relating to, derived from, or generated pursuant to the Agreement, even if generated by Supplier, as well as all data obtained or extracted through ASU's or Supplier's use of such data or information (collectively, ASU Data). ASU Data also includes all data and information provided directly to Supplier by ASU students and employees, and includes personal data, metadata, and user content.

   ASU Data will be ASU's Intellectual Property and Supplier will treat it as ASU Confidential Information (as defined below). Supplier will not use, access, disclose, or license, or provide to third parties, any ASU Data, except: (i) to fulfill Supplier's obligations to ASU hereunder; or (ii) as authorized in writing by ASU. Without limitation, Supplier will not use any ASU Data, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking, or product demonstrations, without, in each case, ASU's prior written consent. Supplier will not, directly or indirectly: (x) attempt to re-identify or de- aggregate de-identified or aggregated information; or (y) transfer de- identified and aggregated information to any third party unless that third party agrees not to attempt re-identification or de-aggregation. For ASU Data to be considered de-identified, all direct and indirect personal identifiers must be removed, including names, ID numbers, dates of birth, demographic information, location information, and school information. Upon request by ASU, Supplier will deliver, destroy, and/or make available to ASU, any or all ASU Data.

8. **Nondisclosure and Trade Secrets**. Supplier may receive (or has received) from ASU and otherwise be exposed to confidential and proprietary information relating to ASU's business practices, strategies, and technologies, ASU Data, as well as confidential information of ASU necessary to perform and/or provide the Goods/Services (collectively, ASU Confidential Information). ASU Confidential Information may include, but is not limited to, confidential and proprietary information supplied to Supplier with the legend "ASU Confidential and Proprietary," or other designations of confidentiality. As between Supplier and ASU, the ASU Confidential Information is the sole, exclusive, and valuable property of ASU. Accordingly, Supplier will not reproduce or otherwise use any of the ASU Confidential Information except in the performance or provision of the Goods/Services, and will not disclose any of the ASU Confidential Information in any form to any third party, either during or after the Term, except with ASU's prior written consent. Upon termination of the Agreement, Supplier will cease using, and will return to ASU, all originals and all copies of the ASU Confidential Information, in all forms and media, in Supplier's possession or under Supplier's control.

   Supplier will not disclose or otherwise make available to ASU any confidential information of Supplier or received by Supplier from any third party.

   Supplier will have no obligation to maintain as confidential ASU Confidential Information (other than ASU Data) that Supplier can show: (i) was already lawfully in the possession of or known by Supplier before receipt from ASU; (ii) is or becomes generally known in the industry through no violation of the Agreement or any other agreement between the parties; (iii) is lawfully received by Supplier from a third party without restriction on

disclosure or use; (iv) is required to be disclosed by court order following notice to ASU sufficient to allow ASU to contest such order; or (v) is approved in writing by ASU for release or other use by Supplier.

9. **Privacy; No Waivers or End User Agreements.** Supplier will not require any ASU faculty, staff, or students to waive any privacy rights (including under FERPA or the European Union's General Data Protection Regulation (GDPR)) as a condition for receipt of any Goods/Services, and any attempt to do so will be void. If Supplier requires ASU faculty, staff or students to accept a clickwrap, click-through, end user license, or other similar agreement (End User Agreement), the terms of the End User Agreement that conflict or are inconsistent, with the terms of the Agreement or ASU's Privacy Statement will be void.

10. **Data Protection.** Supplier will ensure that all services undertaken pursuant to the Agreement are performed in compliance with applicable privacy and data protection laws, rules, and regulations. In addition, Supplier is responsible to ASU for compliance with the Agreement by all Supplier Parties. If Supplier will serve as a Processor of ASU Data that includes Personal Data of Data Subjects in the European Union, Supplier will cooperate with ASU to comply with the GDPR with respect to such Personal Data and Data Subjects. This includes ensuring that all Data Subjects have signed appropriate Consents, and signing and complying with all documents and agreements reasonably requested by ASU, including any data processing agreements. All capitalized terms in this section not otherwise defined in the Agreement are defined in the GDPR.

11. **Third Party Arrangements**. From time to time, ASU may enter into arrangements with third parties that may require Supplier to work cooperatively with and/or connect and use infrastructure with third parties. On a case-by-case basis, ASU and Supplier will work cooperatively, timely, and in good faith to take such actions as may be necessary or appropriate to give effect to ASU's third party agreements. Supplier will not be bound to terms and conditions of a third party that are different from this Agreement unless expressly agreed in writing. If the third party terms and conditions conflict with this Agreement's terms, impact Supplier's ability to meet service level agreements of this Agreement, or may cause Supplier to incur additional costs, then the parties will enter into good faith negotiations for an amendment to this Agreement prior to Supplier agreeing to compliance with the third party terms and conditions.

IN WITNESS WHEREOF, the parties have signed this Agreement as of the Effective Date.

Arizona Board of Regents for and on behalf of Arizona State University	**Supplier**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date Signed: _____	Date Signed: _____

Exhibit A – Description of Deliverables

Exhibit A – Description of Deliverables

This Exhibit A is subject to and made in accordance with the Construction Supplier License and Access Agreement between ASU and Supplier (the Agreement). All capitalized terms not defined herein have the meaning in the Agreement. To the extent any provisions of this Exhibit A conflict with the provisions of the Agreement, the provisions of the Agreement will control. Any other terms provided by Supplier or on Supplier's website are expressly rejected.

Equipment Description	Quantity	Price
Total License Fees:		
Services Description	**Services Term**	**Price**
Total Maintenance Fees:		
Supplier will provide service levels per the Service Level Agreement in this Exhibit A.		

Additional Terms:

Service Level Agreement:

List any Attachments (including Equipment Warranties) **(**include number of pages of each)**:**

Arizona Board of Regents for and on behalf of **Arizona State University**

By: _____

Name: _____

Title: _____

Date Signed: _____

Supplier

By: _____

Name: _____

Title: _____

Date Signed: _____