DATA PRIVACY AND SECURITY ADDENDUM (EFFECTIVE 01.01.2021)

This Data Privacy and Security Addendum (this "**Addendum**") applies to and is incorporated by reference into all Purchase Orders (the "**Agreement**") between Motiva Enterprises LLC and/or its affiliated companies (the "**Company**") and vendors, suppliers and contractors (the "**Contractor**"). The provisions of the Agreement shall be interpreted to give meaning to all appendices and exhibits, provided, however, in the event of any conflict between the Agreement and this Addendum, this Addendum shall control. Capitalized terms used but not defined in this Addendum shall have the meaning specified in the Agreement. In addition to the requirements of the Agreement related to data privacy and/or security, Contractor agrees to the following provisions:

1. **Contractor Requirements.** Contractor shall:

   A. Protect Personal Data and Company Data (collectively referred to as "**Data**" in this Addendum) from unauthorized access and disclosure at all times and in accordance with highest industry standards and best practices. "**Personal Data"** shall any information relating to an identified or identifiable individual, unless otherwise defined under Applicable Laws related to the protection of individuals, the processing of such information, and security requirements for and the free movement of such information. "**Company Data**" shall mean any and all information, data, materials, works, expressions or other content, including any that are (a) uploaded, submitted, posted, transferred, transmitted or otherwise provided or made available by or on behalf of Company or any authorized user for processing by or through the hosted services, or (b) collected, downloaded or otherwise received by Contractor or the hosted services for Company or any authorized user pursuant to the Agreement or any Purchase Order or at the written request or instruction of Company or such authorized user. All output, copies, reproductions, improvements, modifications, adaptations, translations and other derivative works of, based on, derived from or otherwise using any Company Data are themselves also Company Data;

   B. Comply with all Applicable Laws relating to the processing of Data and matters connected therewith and incidental thereto, including but not limited to the (1) all United States federal and state laws, statutes, codes, ordinances, rules and regulations, writs, orders, directives, judgments, and decrees pertaining to the privacy, confidentiality, handling, storage, data export, disposal, and/or safeguarding of customer, employee, financial, health, or other personal information, records, or data, and any breach notification and incident response laws and regulations related thereto (2) European Union's General Data Protection Regulation (EU) 2016/679 ("GDPR"); (3) Canada's Privacy Act and the Personal Information Protection and Electronic Documents Act ("PIPEDA") and any other Canadian federal or provincial laws pertaining to information or data security, privacy, breach notification and incident response laws and regulations;

   C. Restrict access to Data to Contractor employees with a direct need to know the contents of Data;

D. Require all Contractor employees with access to Data to execute a confidentiality agreement (in writing and adequately protecting the disclosure of Data) or ensure they are under an appropriate statutory obligation of confidentiality;

E. Ensure that any third-party vendor or service provider that is engaged by Contractor to process, store, transfer or otherwise use or have access to the Data on Contractor's behalf has entered into a written contract that meets the requirements under this Addendum and otherwise in compliance with Applicable Laws. Notwithstanding, any services provided by a third-party vendor or services provider engaged by Contractor shall be deemed to have been provided by Contractor, and Contractor shall be directly liable and responsible to Customer for all acts and omissions resulting in a Security Incident.

F. Not transfer Data across borders (i.e. from one country or legally recognized international jurisdiction to another) or store Data outside of the United States without written authorization from Company, unless required to do so by Applicable Laws;

G. Not use Data for any reason other than to the extent required to perform the Services under the Agreement;

H. Implement and maintain security controls ("Security Controls") in accordance with generally accepted industry standards and best practices and in compliance with Applicable Laws to ensure the security and confidentiality of any Data; protect against any anticipated threats or hazards to the security or integrity of any Data; and protect against unauthorized access to, and loss, destruction, theft disclosure and/or use of, any Data that could result in substantial harm or inconvenience to Company. Contractor must ensure that Data is processed, transferred and/or stored on secure networks and systems having the following controls at a minimum:

i. All Data must be housed in a physically & environmentally secure facility that has completed attestation reports, audit reports or external certifications (or industry standard successor or equivalents) which are based on certification requirements undertaken annually in compliance with such certifier's requirements, and upon reasonable written notice, provide Company with a copy of its most recent certification and/or audit report.

ii. All software provided by Contractor to Company for purposes of installation into the Company's network, must be scanned at Contractor's expense and proper reporting of scan results provided to Company prior to installation. The following scan types are required.

1.H.ii.1. Code Scanning

1.H.ii.2. Vulnerability/Malware scanning

iii. External access to all networks and systems must be protected by firewalls and intrusion prevention systems used to limit/filter network traffic; logging and monitoring systems; access control systems and encryption.

iv. All networks and systems must be securely configured to reduce unauthorized access and denial of service vulnerabilities and updated at least monthly with security patches and daily with anti-malware software.

v. A disaster plan must be in place to ensure continuous access to Data except for time during which a Force Majeure event is ongoing.

vi. Daily backups must be created to ensure system and Data is fully recoverable, even if a Force Majeure event occurs. Backup files of Data must be moved at least weekly to a secure facility in another time zone.

vii. Evaluate and adjust its Security Controls to: (i) address any changes or additions to the services, its operations, or the relationship between the parties; (ii) address any risks or vulnerabilities reported to or discovered by Contractor; (iii) meet evolving industry standards; (iv) comply with and respond to any changes in Applicable Laws; and (v) address any other and promptly correct any material deficiencies or vulnerabilities identified as part of any monitoring, testing, or auditing.

I. Perform a criminal background check on all individuals with potential access to Data that includes:

i. Verification of legal authority to work in the U.S.

ii. Review of the individual's record of criminal conviction history in jurisdictions in which the individual resided or worked for more than 30 days within the past seven years to ensure that such individual has not been convicted of a felony offense within the past seven (7) years; or any misdemeanor related to violent crimes, property offense, substance abuse, or fraud.

iii. Criminal conviction history checks must include a review of all federal, state and local criminal conviction records. For purposes of this schedule, the term "criminal conviction" includes probation, deferred adjudication and no-contest pleas.

J. Ensure that access is revoked immediately for those Contractor employees who no longer have a direct need to know the contents of Data;

K. Ensure that it has no information that indicates an individual may pose a risk to Company; and

L. Keep a record of any disclosure of Data that is made for a minimum period of six months, unless an Applicable Law provides otherwise. This record will include: (i) the names and addresses of the third parties to which Data was disclosed; (ii) a detailed description of the Data which was disclosed; and (iii) the date and time on which Data was disclosed.

2. Security Incident. Contractor shall notify Company in writing within twenty-four (24) hours of any known breach of confidentiality or security affecting Company and/or its Data including any known unauthorized access to or misuse, loss, alteration or destruction of Data (each a "Security Incident"). Contractor shall cooperate in taking all reasonable actions necessary to investigate, respond to, and limit the adverse effects of the Security Incident, and shall reasonably participate in Company's internal incident response plan where applicable. Contractor shall coordinate with Company regarding any notifications to regulators, law enforcement, affected individuals, and the press. In the event of a breach by Contractor of this Section 2 resulting in the unauthorized use or disclosure of Personal Data, Contractor shall, at its own expense, send notices as required by Applicable Law, and provide affected individuals with credit monitoring services where generally available for a specific period not to exceed twelve months, to the extent the breach could lead to a compromise of affected individuals' credit or credit standing.

3. **Payment Card Industry Data Security Standards (PCI DSS) Compliance.** In the event Contractor has access to any credit card information obtained while providing Services to Company (the "Cardholder Data") or Cardholder Data stored in any database or spreadsheet, Contractor will adhere to current PCI DSS requirements and is responsible for the security of that Cardholder Data. The PCI DSS requirements can be viewed at https://www.pcisecuritystandards.org/.

4. **Employee Security.** All Contractor employees who access Data will do so by individual user accounts using strong passwords containing at least eight characters with both letters and numbers used. All Contractor employees must complete annual security awareness training at least annually.

5. **Return or Destruction.** Upon termination of the Agreement or otherwise at the request of Company, the Contractor shall promptly deliver to Company all Data, without retaining copies thereof, unless otherwise required under Applicable Laws. Data will be returned to Company in a format designated by Company and within thirty (30) days of termination or expiration of this Agreement or Company's request. If Company requests secure disposal of Data, Contractor will provide Company written certification of destruction showing that the Data was securely destroyed/wiped in accordance with NIST standards for media sanitization (NIST Special Publication 800-88, Appendix A).

6. **Security Service Level.**

   A. Contractor will have staff on duty and at its site 24x7 that is capable of identifying, categorizing, and responding to a security incident;

   B. Contractor will notify Company of any new potential security vulnerability within four (4) hours of discovery. This notification will include the probable risks associated with the vulnerability;

   C. Contractor will implement a security fix across the application within four (4) hours of approval from Company;

   D. Contractor will notify the Company within fifteen (15) minutes if Contractor believes that an attack is in process;

   E. Contractor will shut down all access to any subscription services or any component of it associated with the subscription services within fifteen (15) minutes upon request of the Company; and

   F. Contractor will assist Company in preparing written responses to audit requirements or findings without charge.

7. **Audit.** Contractor represents and warrants that it has successfully passed a SSAE 18 SOC 1 Type II or a SOC 2 Type II audit within the past twelve (12) months and will provide the documented audit results, including any requested bridge letters to Company, no later than fifteen (15) days after execution of the Agreement. Contractor will conduct and pass a SSAE18 SOC 1 Type II or a SOC 2 Type II audit every twelve (12) months during the term of the Agreement. Failure by Contractor to pass the audit or to provide the audit results or requested bridge letters to Company within fifteen (15) days after receiving the results or upon request from the auditor will constitute a material breach of the Agreement.

8. **Insurance Requirements.** During the term of the underlying Agreement, Contractor will procure and maintain Internet Liability and Network Protection (Cyber risk) coverage in the amount of

$1,000,000 for each claim or wrongful act and shall add "Motiva Enterprises, LLC" as additional insured. The insurance must cover the computer network security breaches that would result in a denial of services, implementation of malicious code, theft or unauthorized destruction of Data and unauthorized access. The insurance policy will, to the fullest extent allowable by law, include a waiver of subrogation in favor of Company and Affiliates, and any of their respective officers, directors, employees and borrowed servants. Upon Company's request, Contractor will provide Company with evidence of such insurance.

9. **Limitation of Liability.** Nothing contained in the Agreement or this Addendum, excludes, limits or caps Contractor's liability for (i) breach of Applicable Laws, (ii) a Security Incident, or (iii) failure to comply with this Addendum.

10. **Termination.** In the event of a material breach of this Addendum, Company may immediately terminate the Agreement for Contractor default.

11. **INDEMNITY. CONTRACTOR SHALL DEFEND, INDEMNIFY, RELEASE, REIMBURSE AND HOLD HARMLESS COMPANY FROM AND AGAINST ANY AND ALL LIABILITIES, DAMAGES, CLAIMS, DEMANDS, CAUSES OF ACTION, FINES, AND LOSSES AND EXPENSES (INCLUDING REASONABLE ATTORNEYS' FEES, EXPERT FEES AND LITIGATION COSTS) OF EVERY KIND AND CHARACTER INCLUDING WITHOUT LIMITATION ALL LOSS, DAMAGE AND DESTRUCTION OF PROPERTY, LOSS OF IDENTITY OR CREDIT INFORMATION, CORRUPTION OR DESTRUCTION OF DATA ARISING OUT OF OR RELATED TO (A) A SECURITY INCIDENT TO THE EXTENT CAUSED BY OR THE FAULT OF CONTRACTOR; AND (B) CONTRACTOR'S, OR ITS AGENTS OR EMPLOYEES' FAILURE TO COMPLY WITH ANY OF THE OBLIGATIONS SET FORTH IN THIS ADDENDUM, INCLUDING, WITHOUT LIMITATION, FAILURE TO COMPLY WITH APPLICABLE LAWS**