PURCHASE ORDER TERMS AND CONDITIONS

General Purchase Conditions of Capgemini

Version December 2017

1. General Terms. Vendor shall provide to Capgemini the Services Work Product (as defined below) and/or Goods in accordance with the requirements in the specifications for such Services, Work Product and Goods in the Purchase Order to which these terms and conditions relate (collectively, "Purchase Order"). "Work Product" shall mean the materials that are prepared or developed by Vendor in connection with performing Vendor's obligations under this Purchase Order, and shall include all information, data, material, discoveries, ideas (whether or not patentable or reduced to practice), concepts, software in various stages of development, designs, drawings, specifications, techniques, models, data, algorithms, documentation, diagrams, flow charts, methods, techniques, research, processes, procedures, know-how, marketing and development plans, techniques and materials, and all tangible embodiments of each of the foregoing (in whatever form and media) and all intellectual property appurtenant to or inherent in the same. This Purchase Order, which includes the terms of the Supplier Standards of Conduct and Compliance Management Requirements found at https://www.capgemini.com/resources/capgemini-supplier-standards-of-conduct-compliance-management-requirements, constitutes the entire agreement between Capgemini and the Vendor with respect to the subject matter hereof, and supersedes any and all prior or contemporaneous written or oral communications between the parties. Terms and conditions different from or in addition to those set forth in this Purchase Order, including, but not limited to any terms contained in Vendor's quote, invoice or other communication shall not be binding on Capgemini unless agreed to in writing by an authorized representative of Capgemini. The terms and conditions of this Purchase Order shall supersede any of Vendor's terms, whether attached or not. Any document or form or letter of acknowledgement prepared by Vendor which is inconsistent or conflicts with any of the terms and conditions of this Purchase Order shall be deemed a counteroffer, void, and of no effect and this Purchase Order shall govern. Notwithstanding the above, in the event that there is a pre-existing, mutually executed, binding agreement ("Existing Agreement") between the parties, the terms and conditions of the Existing Agreement shall supersede the terms and conditions of this Purchase Order unless explicitly overridden by the parties in writing.

2. Termination. Capgemini may terminate for convenience this Purchase Order at any time, in whole or in part by written notice.

3. Acceptance. If Capgemini, in its sole and reasonable discretion, determines that the Services performed or the Work Product or Goods delivered by Vendor do not conform to the specifications or the standards or other acceptance criteria agreed to by the parties, Capgemini shall notify Vendor thereof, specifying in reasonable detail the respects in which the Services or Work Product are unsatisfactory or unacceptable. Within five (5) days (or such time as is agreed in writing by the parties) following receipt of any such notice, Vendor shall, at no additional cost to Capgemini, take all steps necessary to render the Services and Work Product satisfactory and acceptable to Capgemini within the time period set forth above.

4. Changes to Services. If at any time Capgemini desires to modify any of the Services (or requirements related thereto) or to request new or additional services, Capgemini may submit a Change Order to the Vendor, describing the desired change in reasonable detail, to which the Vendor shall promptly respond in good faith. A Change Order shall take effect upon the mutual written agreement of the parties. Any additional work performed by Vendor without an effective Change Order will not entitle Vendor to increased compensation.

5. Compensation/Records. Unless otherwise agreed, Capgemini shall pay for any Services, Work Product and Goods upon completion or delivery and forty-five (45) days after Capgemini's receipt of an undisputed invoice. All currency amounts are expressed in Canadian dollars. Vendor shall keep and maintain complete and accurate accounting records in accordance with generally accepted accounting principles to support and document all amounts becoming payable to Vendor hereunder. Upon request from Capgemini, Vendor shall provide to Capgemini access to such records for the purpose of auditing such records. Vendor shall retain all records required under this Section for six (6) years after the amounts documented in such records become due.

6. Taxes. To the extent set forth as a separate item or line item on the applicable invoice, Capgemini shall reimburse Vendor for any sales tax, value added tax (including GST and HST), use tax, or similar tax imposed by any federal, provincial or municipal governmental entity for items and/or services provided under this Purchase Order, excluding taxes based on Vendor's income or property.

7. Confidentiality. "Confidential Information" means the proprietary and confidential information of Capgemini, whether or not specifically identified as "Confidential", including, without limitation, all Work Product, all other information, and know-how that: (i) derives economic value, actual or potential, from not being generally known to or readily ascertainable by other persons who can obtain economic value from the disclosure or use of the information, (ii) is the subject of efforts Capgemini or owner of the third party Confidential Information that are reasonable under the circumstances to maintain the secrecy of the information. Notwithstanding the foregoing, the following information shall not be deemed to be Confidential Information if Vendor's written records show that such information:
(a) was disclosed to Vendor at any time by a third party without violation of any obligation of confidentiality; (b) became known to the general public without any violation of an obligation of confidentiality; or (c) was developed by any employee of Vendor who had no access to any information disclosed to Vendor under this Purchase Order.

Vendor shall use the Confidential Information solely to perform its obligations under this Purchase Order and shall not disclose the Confidential Information other than: (a) to Vendor's personnel, which means employees, subcontractors, agents and representatives (collectively, "Personnel") on a strict "need to know" basis for the performance of their obligations under this Purchase Order and who have entered into written agreements with Vendor containing terms and conditions at least as restrictive as those contained in this Purchase Order; or (b) as required by law or court order, provided that Vendor (i) shall provide immediately to Capgemini written notice of the same; and (ii) shall permit Capgemini to take all reasonable actions to prevent such disclosure, to limit the scope of same and to obtain protective orders to protect the confidentiality of such Confidential Information.

Vendor shall use its best efforts, and in no event no less than the same efforts Vendor uses to protect its own valuable proprietary information and data, to maintain the confidentiality of the Confidential Information. Upon Capgemini's request and upon any termination or expiration of this Purchase Order, Vendor shall promptly return to Capgemini or, if so directed by Capgemini, destroy all tangible embodiments of the Confidential Information (in every form and medium) and certify such return or destruction in writing. This clause shall survive expiration or termination of this Purchase Order. Capgemini would suffer immediate and irreparable harm from any breach of this Section 6 and monetary damages would be inadequate to compensate Capgemini for such harm. Therefore, in addition to any other remedies available to Capgemini at law or in equity, Capgemini shall be entitled to injunctive relief for any such breach without posting of bond or other security and without proof of actual damages.
Vendor and their contractors and employees will maintain confidentiality with regard to all Capgemini confidential and business sensitive information (usually under a Non Disclosure Agreement) they have access to, in accordance with applicable laws or applicable contractual engagement. Vendor will protect all intellectual property belonging to Capgemini, our customers, other Suppliers and individuals.

8. Warranties. Vendor represents, warrants and covenants that (i) all Services provided by Vendor will be performed in a good, workmanlike, timely and professional manner by qualified persons fully familiar with the requirements for the Services and the materials and technology to be used to perform the Services; (ii) all Goods provided will be new and will not be used or refurbished and that all Goods delivered shall be free from defects in materials and workmanship and shall conform to all applicable specifications; (iii) all Work Product shall be of original development by Vendor or Vendor has obtained all rights necessary to transfer such Work Product to Capgemini to perform its obligations hereunder; (iv) Vendor's Personnel shall, comply with all notices and instructions regarding the use of equipment and maintenance of the same that are provided by the manufacturer of such equipment; and (v) the Services and the Work Product shall not infringe upon the Confidential Information, copyrights, patents, trademarks, trade secrets and other intellectual property rights (collectively, "Intellectual Property") of Capgemini or any third party. During the ninety (90) day period commencing on the date that Capgemini accepts any particular Services, Work Product or Goods, such Services, Work Product or Goods shall conform to, and perform in accordance with, any applicable Specifications and shall otherwise be free from any material defects. After such ninety (90) day period, corrections and remedies, if any, shall be furnished on a time and materials basis at Vendor's then current charges at the request of Capgemini.

9. Vendor Personnel. Capgemini may require that Vendor replace any of Vendor's Personnel which Capgemini deems to be unacceptable with other Personnel meeting the requirements of Capgemini. No independent or dependent contractors may be used without first securing written permission from Capgemini. Capgemini's right hereunder to require reassignment and replacement of Vendor's Personnel shall not in any way limit Vendor's obligation to perform under this Purchase Order. Vendor shall maintain continuity in Vendor's Personnel assigned to perform work under this Purchase Order and, except as provided above, shall not reassign any such Personnel prior to completion of their respective responsibilities without Capgemini's consent, which shall not be unreasonably withheld. Vendor shall be responsible for the performance of the services and all of the other liabilities and obligations of the Personnel under this Agreement.

10. Ownership. The Work Product (including all intermediate and partial versions thereof) and all Intellectual Property inherent in any of the foregoing or appurtenant thereto, shall be the sole property of Capgemini, and except as expressly specified this Section, Vendor hereby assigns, and shall assign, to Capgemini all right, title and interest in each of the foregoing. All s copyrightable works, as well as all copies of such works, shall be owned exclusively by Capgemini on their creation, and Vendor hereby expressly disclaims any interest in any of them. At all times during the term of this Purchase Order and thereafter, Vendor shall assist Capgemini in protecting its ownership of the Work Product. Vendor agrees to execute and deliver all documents and provide all testimony reasonably requested by Capgemini in connection therewith, and irrevocably designates and appoints Capgemini its agent and attorney-in-fact to act for and in its behalf to execute, register and file any applications, and to do all other lawfully permitted acts, to further the registration, prosecution and issuance of copyrights or similar protections with the same legal force and effect as if executed by Vendor.

11. License to Proprietary Materials. Vendor hereby grants to Capgemini a perpetual, irrevocable, non-exclusive right and license, as required to use fully and completely the Services and the Work Product, to use all Intellectual Property in proprietary materials owned by Vendor or for which Vendor has the right to grant such rights and licenses (including, without limitation, a license to authorize others to do any of the foregoing). Vendor acknowledges that Capgemini may designate third parties to exercise any of the rights and licenses granted to the Capgemini under this Section for the benefit of the Capgemini. Vendor shall not provide to Capgemini any proprietary materials for which Vendor does not have the right to grant to Capgemini the rights and licenses contained this section or provide any Services or Work Product that would require Capgemini to use any Intellectual Property other than that to which Vendor grants to Capgemini a license in this Section, without the prior written consent of Capgemini.

12. Indemnification. Vendor shall defend, indemnify and hold harmless Capgemini, its parent(s), subsidiaries and affiliates, and their respective officers, directors, employees, predecessors, successors, assigns and agents, and shall pay, as incurred, all liabilities, damages, costs, fees and expenses (including reasonable legal fees) relating to any third party claim, action, suit or other proceeding: (a) that Work Products constitute an infringement of any patent, copyright, trademark or trade secret; (b) relating to a breach by Vendor of any of its other representations, warranties, agreements or covenants under this Purchase Order; or (c) relating to any act or failure to act by any Vendor Personnel while on the premises of Capgemini.

13. Insurance. Vendor, at its sole cost and expense, shall maintain at all times during the performance of Services hereunder, the following types of insurance with limits not less than the limits set forth below, and shall be responsible for their own deductibles and self-insured retentions.
(a) Commercial General Liability Insurance on an "occurrence basis", with a limit of not less than one million dollars ($1,000,000) combined single limit per occurrence for bodily injury and property damage liability. Coverage shall also include blanket contractual liability covering all indemnity agreements, a broad form property damage coverage endorsement, independent contractors' coverage, premises/operations, products liability, completed operations, and an endorsement naming Capgemini as an "Additional Insured." The Commercial General Liability Insurance shall also include an endorsement providing that the insurance afforded under the Vendor's policy is primary insurance and without contribution from any other insurance maintained by Capgemini.
(b) Umbrella Liability Insurance with a minimum limit of five million dollars ($5,000,000) in excess of the insurance under policies indicated in this section.
(c) Errors and Omissions Liability Insurance covering the liability for financial loss due to error, omission, negligence of employees and machine malfunction in an amount of at least five million dollars ($5,000,000).
(d) Property Insurance covering the full replacement value of any and all property of Capgemini which is in Vendor's care, custody and/or control. Capgemini shall be named as a Loss Payee on the Property Insurance Policy.
(e) Fidelity Insurance covering losses to Capgemini resulting from but not limited to computer crime and electronic funds transfer losses caused by the dishonest acts of Vendor's employees. The policy limit of liability shall not be less than $1,000,000. Capgemini will be named as a Loss Payee on the Fidelity policy.

14. Compliance with Laws and Rules. Vendor and its employees shall perform all obligations under this Purchase Order in compliance with all laws, ordinances, rules and regulations. Capgemini recognizes that local customs, traditions and practices may differ, but expect as a minimum that our Vendors comply with local, national and international applicable laws, including (but not limited to) all anti-corruption, competition, export control, environmental, health and safety, data protection and labour laws and to monitor compliance with applicable laws.. Vendor shall, and shall be responsible for, ensuring that Vendor's Personnel shall, obey all rules and regulations in effect at any premises of Capgemini at which Vendor's Personnel perform Vendor's obligations under this Purchase Order, including, without limitation, all security requirements and all reasonable instructions and directions issued by Capgemini. **During the performance of this Purchase Order, the Vendor agrees to comply with all federal, provincial, and municipal laws respecting discrimination in employment.** Vendor will not discriminate in hiring, compensation, access to training, promotion, and termination of employment or retirement on grounds of social, cultural, ethnic or national origins, religious or other beliefs, caste, gender, marital status, pregnancy status, sexual orientation, disability, age, and trade union membership. Vendors should promote diversity and inclusion. Vendor represents and warrants to Capgemini that Vendor and anyone acting on Vendor's behalf shall not violate and will strictly comply with all applicable anti-bribery/anti-corruption laws, statutes, regulations, ordinances or standards, including but not limited to the Foreign Corrupt Practices Act. Vendor further represents and warrants to Capgemini that Vendor, or anyone acting on Vendor's behalf, shall not directly or indirectly, pay, promise or offer to pay, or authorize the payment of any money or anything of value to any of the following or to any of their officers, employees, agents or representatives:

(i) Capgemini or any of its affiliated companies;
(ii) Capgemini client or prospective client;
(iii) any government, including any department, agency or instrumentality of any government or any government-owned or government controlled entity;
(iv) a candidate for political office, any political party or any official of a political party;
(v) any other person or entity while knowing or having reason to believe that some portion or all of the payment or thing of value will be offered, given or promised, directly or indirectly, to any person or entity described in subsections (i) – (iii) above; or
(vi) any other person or entity;
(vii) for the purpose of influencing any act or decision of any person or entity described above including a decision to do or omit to do any act in violation of the lawful duty of such person or entity, or inducing such person or entity to use his or its influence to affect or influence any act or decision, in order to assist Capgemini or Vendor in the transactions contemplated under this Agreement.

Vendor, or anyone acting on Vendor's behalf, shall not pay any commissions or fees, or grant any rebates to any employee of Capgemini or any employee of an Affiliate of Capgemini SE, nor favor such employees with any offer or giving of gifts, entertainment or hospitality that is more than nominal value as defined by Capgemini policies and Capgemini Supplier Standards of Conduct & Compliance Management Requirements at https://www.capgemini.com/resources/capgemini-supplier-standards-of-conduct-compliance-management-requirements ("Supplier Code"). In addition, Vendor, or anyone acting on Subcontractor's behalf, shall fully comply with the obligations set forth in the Supplier Code and the North America Environmental Policy (found at https://www.capgemini.com/us-en/capgemini-north-america-environmental-policy/).

In addition, no payment will be made to anyone for any reason on behalf of or for the benefit of Capgemini which is not properly and accurately recorded in Vendor's books and records, including amount, purpose and recipient, all of which will be maintained with supporting documentation. Vendor agrees that its books and records relating to transactions contemplated under this Agreement will be subject to audit at reasonable times as necessary to ensure compliance with the foregoing, that it will provide Capgemini all information Capgemini requests so that it complies with the reporting requirements of all anti-bribery laws and standards, and that it will upon request certify its continued compliance with all anti-bribery laws and standards.

Vendor shall comply with all Data Protection Laws (as defined below) and adhere to the following requirements with respect to any Personal Data of Capgemini, its clients and affiliates of Capgemini SE Vendor will protect personal data and comply with all data protection laws. Supplier will secure Capgemini data against unauthorized access or use. The following definitions apply for the purpose of the below provisions:

i. Applicable Data Protection Legislation: means any applicable data protection law and regulation that applies in the context of the Agreement and in particular (i) any Canadian and other laws and regulations relating to the processing of Personal Data applicable during the term of the Agreement, and (i) the European Regulation n° 2016/679 relating to the processing of Personal Data (GDPR), and similar laws within the UK, Switzerland, and/or the European Economic Area, as of its date of application.
ii. Capgemini Personal Data: means any Personal Data (including those related to the Capgemini's employees and/or customers, including Capgemini clients, and/or suppliers) provided or made available to the Vendor by Capgemini or on its behalf, or gathered by the Vendor from Capgemini, its agents, employees, service providers, suppliers or customers, and all data generated, created or compiled on the basis of such data or by using them.
iii. "Data Breach" means any actual or suspected unauthorized or accidental access, use, loss or disclosure of any Capgemini Personal Data (which, for avoidance of doubt, includes all confidential information), or a breach of Vendor's security or information systems that could reasonably be expected to expose any Capgemini Personal Data (including confidential information), to such unauthorized access, use, loss, or disclosure.
iv. "Data Controller" means the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of Personal Data or as otherwise defined by Applicable Data Protection Legislation;
v. "Data Processor" means any entity acting on behalf of the Data Controller or as otherwise defined by Applicable Data Protection Legislation;
vi. "Data Subject" means an identified or identifiable natural person or as otherwise defined by Applicable Data Protection Legislation.
vii. Personal Data: means any data which can be used to distinguish or trace an individual's identity alone or when combined with other personal or identifying information which is linked or linkable to a specific individual or is otherwise defined as personal data under Applicable Data Protection Legislation.

PROCESSING OF CAPGEMINI PERSONAL DATA

i. In accordance with all Applicable Data Protection Legislation and, in particular, Article 28 of the GDPR or similar legislation, the Parties are entering into this Section to the extent that the Vendor, acting as a Data Processor, processes Capgemini Personal Data on behalf of Capgemini.
ii. In respect of the processing of Capgemini Personal Data, the Parties acknowledge that Capgemini is the Data Controller, and the Vendor is a Data Processor and agree to comply with all corresponding obligations applicable as per Applicable Data Protection Legislation. Annex A sets out main characteristics of the processing. The Parties agree that this Annex may be further completed in writing, subject to a common agreement of the Parties.

a) process the Capgemini Personal Data only on documented instructions from Capgemini and for the sole purposes as defined and agreed by Capgemini, unless required to do so by applicable law to which the Vendor is subject; in such a case, the Vendor shall inform Capgemini of that legal requirement before processing, unless that law prohibits such information on grounds of public interest;
b) ensure that persons authorized to process the Personal Data (i) are bound by confidentiality obligations (ii) have committed themselves to only access, use, disclose, or otherwise process Personal Data in accordance with this Section and for the sole purposes as expressly defined by Capgemini, (iii) have received from the Vendor appropriate training with respect to the correct handling of Personal Data so as to minimise the risk of an accidental Data Breach, and process Personal Data in compliance with the requirements of Applicable Data Protection Legislation;
c) implement appropriate technical and organizational measures to protect the Capgemini Personal Data from a Data Breach according to Capgemini's instructions (at a minimum, such measures shall include the measures identified in Annex B);
d) upon becoming aware of a Data Breach, inform Capgemini, without undue delay but no later than 24 hours after becoming aware of the Data Breach, and provide all such timely information and cooperation as Capgemini may require in order to fulfil their Data Breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Legislation. At a minimum, the Vendor shall provide the following information to Capgemini: (i) the identity and contact details of the data protection officer or other contact point where more information can be obtained; (ii) the nature of the Data Breach, including the categories and number of Data Subjects and the Personal Data concerned by the Data Breach; (iii) a description of the measures Capgemini could take to mitigate the possible adverse effects of the Data Breach and to prevent from another potential Data Breach; (iv) the consequences of the Data Breach; (v) the measures proposed or taken by the Vendor following the Data Breach, including to prevent from any new occurrence. In addition, the Vendor shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Data Breach and shall keep Capgemini up-to-date about all developments in connection with the Data Breach. In any case, Capgemini shall first approve any public communication and/or official notification to competent authority or to Data Subjects regarding such potential or actual Data Breach;
e) assist Capgemini, by appropriate technical and organisational measures, at no additional cost for Capgemini, with the fulfilment of Capgemini's obligation to respond to requests regarding Data Subjects' rights, inter alia: (i) requests from Data Subject's; and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of the Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to the Vendor, the Vendor shall promptly inform Capgemini and within a maximum of five (5) business days, providing full details of the same, and shall, in any case, refrain from responding directly to the Data Subject without Capgemini's prior consent;
f) provide Capgemini with all such reasonable and timely assistance that may be required in order for Capgemini to conduct a data protection impact assessment;
g) at the choice of Capgemini and according to its instructions, delete or return all the Personal Data to Capgemini in a format and on a media determined by Capgemini, upon request from Capgemini after the end of the provision of Services, and deletes existing copies, including any Personal Data sub-processed by a "Vendor's sub-processor", and provide evidence to Capgemini that it has done so, unless Applicable Data Protection Legislation requires storage of the Personal Data, in which event Vendor shall isolate and protect the Personal Data from any further processing except to the extent required by such law. In case of return to Capgemini, following Capgemini's issuance of a receipt of acknowledgement of the restitution, the Vendor shall destroy all Personal Data relating to Capgemini Personal Data) within forty-eight (48) hours after the issuance of the above-mentioned Capgemini's receipt and provide evidence to Capgemini that such destruction took place. Should the law prevent the Vendor from deleting all or part of the Personal Data, the Vendor shall inform Capgemini of such requirements and implements, at its cost, the appropriate anonymization or pseudo-anonymization measures;
h) make available to Capgemini (or its appointed third party auditors) all information, systems and staff, as well as those of any approved sub-processor, necessary to demonstrate compliance with the obligations laid down in this Section and allow for and contribute to audits, including inspections conducted by Capgemini or another auditor mandated by Capgemini, in accordance with the provisions of the Agreement related to audits;
i) not rely on a sub-processor without Capgemini's prior express approval and impose on the approved sub-processor the same data protection obligations as set out in this Agreement, by way of a written contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements defined under this Agreement and entitling Capgemini to carry out appropriate reviews and inspections at the sub-processor's premises or to have them carried out by third parties. Notwithstanding the above, where the sub-processor fails to fulfil its data protection obligations, the Vendor shall remain fully liable to Capgemini for the performance of the sub-processor's obligations. The contract with the sub-processor must clearly define and distinguish the responsibilities of the Vendor and sub-processor; if several sub-processors are used, this shall also apply to the responsibilities between these sub-processors. Any sub-processors authorized by Capgemini for the processing of Capgemini Personal Data as necessary for the performance of the purposes expressly defined by Capgemini under this Agreement (the "Vendor's Authorized sub-processor(s)") are listed in Annex A. The Vendor's appointment of a sub-processor and/or replacement of a Vendor's Authorized sub-processor, is subject to prior written consent of Capgemini. If the Capgemini refuses to consent to the Vendor's appointment of a sub-processor and/or replacement of Vendor's Authorized sub-processor on grounds relating to the protection of the Personal Data, then either the Vendor will not appoint the sub-processor and/or replace the Vendor's Authorized sub-processor, or Capgemini may elect to suspend or terminate the Agreement under the conditions defined under the Termination Section of the Agreement;
j) Immediately inform Capgemini if, in the Vendor's opinion, an instruction of Capgemini, infringes any Applicable Data Protection Legislation;
k) In the event that the Vendor intends to process Personal Data from the European Union, the UK, Switzerland, and/or the European Economic Area ("EEA") to a country outside of the foregoing (**Third Country**), the Vendor shall obtain Capgemini's prior express written consent. The Vendor shall request such prior consent by providing Capgemini with a reasonable prior notice and with all relevant information relating to the purpose of such transfer and the country where the Personal Data would be transferred;
l) Any transfer of Personal Data approved by Capgemini, shall be made possible only to the extent that an appropriate level of protection is provided for the Personal Data transferred, as approved by Capgemini. This can be achieved by entering into standard clauses as may be adopted by the European Commission and/or competent data protection authorities or by relying on binding corporate rules of the Vendor and/or of the sub-processor duly approved by the competent data protection authorities. In any case, the Vendor shall assist Capgemini with ensuring that the above-mentioned measures are actually implemented and shall refrain from transferring Personal Data to a Third Country before any such measures are actually implemented and approved by Capgemini;
m) In addition, the Vendor acknowledges that Capgemini has approved Binding Corporate Rules for Controller and Processor (all together, "the Capgemini BCRs"). Consequently, Capgemini requires the Vendor to abide by data protection standards equivalent to those described in the Capgemini BCRs. The Capgemini BCRs, available at https://www.capgemini.com/resources/capgeminin-binding-corporate-rules/ are inserted by reference into this Agreement and can be sent to the Vendor by electronic means on request; and

iii. The Vendor shall:

n) In addition to the obligations set forth in this Exhibit 1, Vendor shall also comply with any particular requirements of Capgemini, as described in this Agreement

15. Governing Law. This Purchase Order shall be governed by and construed in accordance with the laws of the Province of Ontario , without reference to its choice of law principles. Any action pursuant to or arising from this Purchase Order shall be brought in a court in Toronto, Ontario.

16. Assignment and Subcontracting. Vendor shall not assign or subcontract its rights and obligations under this Purchase Order without obtaining Capgemini's prior written consent. Any permitted subcontractors shall agree in writing to be bound by the terms of this Purchase Order.

17. Time is of the Essence. Vendor acknowledges that time is of the essence in performing its obligations hereunder.

18. Independent Contractor. Vendor is engaged only for the purpose and to the extent set forth in this Purchase Order, and its relation to Capgemini shall be that of an independent contractor. Vendor Personnel are not, and shall not be considered, employees of Capgemini for any purpose whatsoever.

19. Publicity. Vendor agrees that Capgemini's name will not be used in any written advertising or marketing promotion of Vendor except with Capgemini's prior written consent.

20. Force Majeure. Neither party shall be liable for failure to comply with any of the terms of this Purchase Order if and to the extent that such failure has been caused solely by fire, war, insurrection, epidemic, government restrictions, force majeure or other causes beyond the control and not due to the fault of the non-performing party, provided the non-performing party shall promptly give notice to the other party and shall exercise all reasonable efforts to resume performance. If the non-performance continues for more than thirty (30) days, the party whose ability to perform has not been so affected may, by giving written notice, terminate this Purchase Order.

21. Language. The parties confirm their express wish that this Agreement and all documents related thereto be drawn up in English. Les parties confirment leur volonté expresse de voir la présente convention et tous les documents s'y rattachant être rédigés en anglais.

ANNEX A - DESCRIPTION OF PERSONAL DATA PROCESSING
THIS INFORMATION SERVES AS A BASIS FOR COMPLIANCE WITH ARTICLE 30.2 GDPR

Name of the Data Protection Officer

Capgemini	**Processor(s) or Subprocessor(s)**
Aaron Fontenot (or his successor)	[insert name of DPO for processor(s) or subprocessor(s)]

Individuals

The Personal Data concern the following categories of Data Subjects:

Categories of Data Subjects	**Strike through if not applicable**
(potential)/(ex) customers	yes/no
applicants and (ex) employees, interns	yes/no
(potential)/(ex) suppliers	yes/no
(potential)/(ex) business partners	yes/no
Any other category: [insert category]	[please specify]

Categories of data

The Personal Data concern the following categories of data:

Categories of data	Strike through if not applicable
Contact data (e.g. name, address, title, position, telephone, e-mail address, etc.)	yes/no If yes, [please specify]
Connection data (e.g. IP address, logs, usernames, passwords, etc.)	yes/no If yes, [please specify]
Contractual data (e.g contractual relationship, order history, order numbers, billing and payment etc.)	yes/no If yes, [please specify]
Official ID data (e.g. copy of passport or national ID), data related to civil status	yes/no If yes, [please specify]
Data pertaining to the personal life of Data Subjects (e.g. life habits, familial situation, etc.)	yes/no If yes, [please specify]
Data pertaining to the professional life of Data Subjects (e.g. CV, professional trainings, certifications, etc.)	yes/no If yes, [please specify]
Economic and Financial Data (e.g. compensation, financial status, tax situation, etc.)	yes/no If yes, [please specify]
Location Data (e.g. travels, GPS data, GSM data, etc.)	yes/no If yes, [please specify]
Any other category: [insert category]	yes/no If yes, [please specify]

Special categories of data (if applicable)

The Personal Data concern the following special categories of data:

Special categories of data	Strike through if not applicable
Personal data of children	yes/no If yes, [please specify]
Any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, criminal records and personal data regarding unlawful or impeding behavior with regard to an imposed prohibition for that behavior. Examples are photos, film images, medical data etc.	yes/no If yes, [please specify]

Processing: purposes of the processing of Personal Data

Duration: specify the duration of the processing of Personal Data

Transfer of personal data to third countries

Country(ies) outside of the European Economic Area (EEA) where Personal Data is transferred	

Subcontractor list of internal sub-processors:

Name of Internal sub-processor(s)	**Country location**	**Country(ies) of processing**	**Contact details**
[insert name of Internal sub-processor]	[insert country location of Internal sub-processor]	[insert country(ies) of processing of Internal sub-processor, if any]	[insert contact details of Internal sub-processor]

Subcontractor list of external sub-processors:

Name of External sub-processor(s)	**Country location**	**Country(ies) of processing**	**Contact details**
[insert name of External sub-processor]	[insert country location of External sub-processor]	[insert country(ies) of processing of External sub-processor, if any]	[insert contact details of External sub-processor]

Annex B – technical and organizational security measures

The Vendor shall implement and maintain the appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity and availability of the data that it receives, maintains, stores, processes or transmits on behalf of Capgemini.

The Vendor must have, but not limited to, the below technical and organizational security measures:

1. General.

a. Information security policies and procedures are formulated, developed and implemented with governance model with specified function and a person is accountable for information security implementation.
b. The information security policies, procedures and implementations are reviewed by the Vendor at appropriate management level.

2. Information security policy.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce:

a. an on-going program of information security policies, security procedures, and security technical controls;
b. a security incident management program;
c. a security awareness program;
d. business continuity and recovery plans, including regular testing;
e. rigorous change control procedures; and
f. procedures to conduct periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for timely remediation

3. Access and authentication.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce:

a. appropriate mechanisms for user authentication and authorization in accordance with a "need-to-know" policy to the Vendor systems supporting Capgemini's business;
b. controls to restrict access to the Vendor systems for remote users, contractors and suppliers;
c. timely and accurate administration of user account and authentication management for the Vendor systems;
d. processes to ensure assignment of unique IDs to each person with computer access;
e. processes to ensure Vendor-supplied defaults for passwords and security parameters are changed and appropriately managed on-going;
f. mechanisms to track all access to the data by unique ID;
g. mechanisms to encrypt or hash all passwords;
h. process to promptly revoke accesses of inactive accounts or terminated/transferred users
i. good authentication procedure for protecting its end-points (desktops and laptops); and,
j. controls to protect against the risks of mobile computing and communication facilities.

4. Paper record.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce:

a. a clear desk and clear screen policy.
b. Information, which includes paper documents, handled by the Vendor is classified, labeled, protected and handled per the document classification policy.

5. Electronic communication.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce that:

a. E-mails are automatically scanned by server based anti-virus software.
b. Telecommunications cabling carrying data or supporting information services are protected from interception or damage.

6. Storage of data.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce that:

a. Equipment, information or software are not being taken off-site without Capgemini's prior authorization.
b. Security is applied to off-site equipment considering the different risks of working outside the organization's premises.
c. All items of equipment containing storage media are checked to ensure that any Special Categories of Personal Data (i.e.: Sensitive Personal Data) and licensed software has been removed or securely overwritten prior to disposal.

7. Local user access.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce that:

a. In case the Vendor is working in a multi-tenancy mode, network and data segregation are implemented.
b. Physical access to the Vendor's premises is restricted to authorized personnel.
c. Periodic access review is implemented for both logical (network) access and physical (facilities) access.

8. Security architecture and design.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce that a security awareness program is implemented.

9. ISO certification.

The Vendor warrants that it has established and during the term of this Agreement it will always enforce, unless otherwise agreed in writing with Capgemini, that:

a. The security management system of the Subcontractor is certified or aligned with ISO 27001 and SSAE16/ISAE3402.
b. it shall provide Capgemini's business using SAS 70 Type II certified or ISO27001 certified (or at least equivalent) data centers.

10. Physical access.

The Vendor warrants that it has established enforce during the term of this Agreement and any transition assistance period ("TAP"):

a. physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and protected in appropriate data centers;
b. appropriate facility entry controls to limit physical access to systems that store or process the data;
c. processes to ensure access to facilities is monitored and restricted on a "need-to-know" basis; and
d. controls to physically secure all the data and to properly destroy such information in accordance with this Agreement.

11. Security architecture and design

The Vendor warrants that it has established and during the term of this Agreement it will always maintain:

a. a security architecture that ensures delivery of the appropriate technical and organizational security measures;
b. functionality in Capgemini's business that enables Capgemini to encrypt Personal Data;
c. a system of effective firewall(s) and intrusion detection technologies necessary to protect the data; and
d. data base and application layer design processes that ensure applications are designed to protect the data that is collected, processed, used, stored, accessed, and transmitted through such systems.

12. System and network management.

The Vendor warrants that it has established and during the term of this Agreement and any transition assistance period it will always maintain:

(i) Applicable security patches;
(ii) Processes to monitor, analyze, and respond to security alerts;
(iii) Appropriate network security design elements that provide for segregation of data;
(iv) Use and regular update anti-virus software; and
(v) Processes to regularly maintain, manage and protect the installed software.

a. The data must be securely stored in an ISO 27001 (or any other cloud relevant ISO certification) or SAS-70 certified data center.
b. Any server infrastructure hosting data should be monitored for information security attacks at the network, operating system, database and application level using intrusion detection or prevention systems.
c. Appropriate level of audit logs should be enabled at the network, operating system, and database and application level to detect and investigate security attacks.
d. Vendor must implement industry best security practices to secure network, operating system, database and the web application levels.
e. Vendor must implement and follow patch management process to ensure all software is updated with latest security patches/versions.
f. Vendor must respond to any security incident questions/calls by Capgemini within 24 hours after the receipt of the email or call by Capgemini.
g. appropriate network security design elements that provide for segregation of data;
h. use and regular update anti-virus software.

13. Due diligence/audits.

a. Capgemini reserves the right to perform a security audit if needed at least once a year (for which the Vendor shall allocate appropriate resources to enable Capgemini's audit), or the Vendor shall provide continued assurance regarding the security of Capgemini's business through the performance at least once a year of an independent third party security audit, as well as periodic vulnerability assessments, penetration tests, and internal audits.
b. The audits results and plans for resolving the audit results shall be shared with Capgemini within 30 days of the Vendor's receipt of such audit results. Additionally, Vendor must remediate findings capable of impacting Capgemini's business within mutually agreed timelines.
c. The audit should minimally check for security assessment based on internationally recognized standards (ISO 27001, OWASP top 10, CSA Control Matrix as appropriate).
d. Capgemini may request to perform, at its own expense, an application penetration test of Capgemini's business, which shall be no more than once per year. Capgemini must notify the Vendor in advance of any tests by submitting a request to the Vendor and completing a penetration testing agreement. The Vendor and Capgemini will agree upon a mutually acceptable time for the test, which shall typically be within thirty (30) days of such request. Capgemini shall be entitled to notify the Vendor should Capgemini detect any vulnerability. Upon such notice, the Vendor shall promptly make any necessary changes to secure Capgemini's business.

14. Disaster Recovery.

a. Vendor shall have in place appropriate business continuity and disaster recovery plans based at minimum on the Business Continuity Institute ("BCI") good practice guidelines. Such plans shall be approved by the Vendor's senior management at the level equivalent to a CEO or COO.
b. Vendor shall recover all data and shall provide access to Capgemini's business within the agreed recovery time objective ("RTO").
c. Vendor shall ensure recovery of data until the agreed recovery point objective ("RPO").
d. Vendor shall perform Disaster Recovery tests at least once in a year. The test plans shall be made available to Capgemini upon request.

15. Security breach notification and mitigation.

a. The Vendor agrees to report to Capgemini any security breach in writing without undue delay after being aware and within a maximum of twenty-four (24) hours. In addition, the Vendor shall provide any additional information reasonably requested by Capgemini for purposes of investigating the security breach and any other available information that Capgemini is required to include to the individual under the laws at the time of notification or promptly thereafter as information becomes delayed.
b. In the event of any security breach, the Vendor agrees to promptly cure such security breach and mitigate any harmful effects therefrom. Similarly, if because of any security breach, Capgemini is required by applicable law to notify impacted individuals, the Vendor agrees to reimburse Capgemini's reasonable costs associated with such notifications or, at the Vendor's election, provide the notification directly.