TERMS AND CONDITIONS: SERVICES

1. Parties. The term "Seller" refers to the addressee set forth on the face of Buyer's purchase order, and the term "Buyer" refers to the company set forth as addressor on the face of the purchase order.

2. Terms. The following terms and conditions (including the contents of Schedule "A" attached hereto) apply to all Buyer's purchase orders relating to services, in addition to any terms set forth on the face of an individual purchase order or in any plans, specifications or other documents incorporated by reference (collectively, an "Order"). Acceptance is limited to the terms and conditions of this Order, and no purported revisions of, additions to, or deletions from the Order shall be effective, whether in any proposal, invoice, acknowledgment or bid from Seller or otherwise, and no local, general or trade custom or usage shall be of any force or effect or be deemed to result in any variation herein unless expressly agreed to in writing by Buyer's authorized representative. The furnishing of any services contemplated by this Order shall constitute acceptance by Seller of this Order in strict accordance with all of its terms and conditions.

3. Changes. Buyer may make changes to the Order at any time and Seller shall accept such changes. If a change by Buyer causes an increase or decrease in the cost or time required for Seller's performance, as soon as practicable, the parties shall agree to an equitable adjustment of the purchase price and/or delivery schedule, as applicable, and incorporate such changes as a revision change to the Order. No other form of notification or verbal agreement shall be binding on Buyer.

4. Performance; Inspection; Acceptance. Time of delivery is of the essence. In the event of a delay or default in performance by Seller in accordance with the Order, Buyer may, in its sole discretion, extend the time period for performance, upon conditions satisfactory to Buyer. Any extension granted by Buyer will not prejudice its ability to exercise its termination rights in the event of further delay or default. Alternatively, in such event and notwithstanding Sections 12 or 13, Buyer may terminate this Order in whole or in part, without any further obligation of any nature to Buyer, receive a refund of the corresponding amounts paid to the Seller and seek satisfactory performance by alternative sellers. Any extension granted by Buyer will not prejudice its ability to exercise its termination rights in the event of further delay or default. Payment for or acceptance of nonconforming services shall not constitute an acceptance thereof, limit or impair Buyer's right to assert any legal or equitable remedy, or relieve Seller's responsibility for defects, latent or otherwise.

5. Insurance. Seller shall maintain at its own expense, at all times during the term and any extension of this Order, the following insurance with reputable insurers whose policies are valid in the jurisdiction in which the services are performed: (i) all-risk property insurance under this Order or in respect of the services covered by this Order; (ii) all-risk property insurance in respect of any item owned by the Buyer which is in the custody, control or power of the Seller; (iii) a Commercial General Liability insurance policy, with a coverage limit of five million dollars ($5,000,000.00), inclusive of bodily injury and property damage, for any one occurrence. (iv) third party automobile liability insurance, with a coverage limit of two million dollars ($2,000,000) per occurrence; and (v) professional liability insurance coverage, with a limit of two million dollars ($2,000,000) per occurrence. Seller shall include Buyer as an additional insured under any applicable policies and provide proof of workplace safety insurance approvals in the jurisdiction of the place the services are performed. Seller shall provide Buyer with evidence of such insurance coverage and proof of payment of premiums in respect of such insurance policies upon Buyer's request. Seller shall also maintain at its own expense, at all times during the term and any extension of this Order, responsibility and insurance for risk of loss, theft, damage or destruction to any Seller-owned rental equipment.

.

6. Payment Terms. Payment terms shall be as set forth on the face of Buyer's Order and payment shall be made within such period following receipt and acceptance of the services and receipt, in proper form and substance, of all documentation required by this Order. This Order shall not be filled at any price higher than last quoted or charged by Seller, except as expressly agreed to in writing by Buyer. Seller warrants and agrees that the price and terms provided for the services covered by this Order are no less favorable to Buyer than those offered to Seller's best customer under generally similar circumstances in terms of quantity and delivery schedule. Acceptance by Seller of the final payment will constitute a waiver of all claims by Seller against Buyer except those previously made in writing in accordance with this Order and still unsettled. Payments to Seller, including final payment, will not relieve Seller from any of its obligations or liabilities under this Order or otherwise.

7. Seller's Warranties. Seller warrants that all services shall be provided in a professional and workmanlike manner, with a degree of skill and care consistent with current, good and sound professional procedures and will be delivered in a timely manner and on schedule, as determined by the Buyer. Seller shall always act diligently in the performance of the services. If a breach of warranty occurs, Seller shall re-perform, at the Seller's expense, any portion of the services which are defective until such non-compliance is corrected, without waiving any other rights, return for credit, or replacement of the nonconforming services. Seller's warranties shall survive acceptance and payment and shall run to Buyer, its successors, assigns, customers and users of the services and shall not be deemed to be exclusive.

8. Intellectual Property. To the fullest extent permitted by law, Seller shall indemnify and hold harmless Buyer, and its affiliates, and their respective officers, directors, agents, shareholders, employees, representatives, suppliers and subcontractors, successors and assigns, and all customers and users of any service of any of them ("Indemnified Parties") from and against any and all losses, liabilities, claims, demands, costs and expenses (including reasonable lawyers' fees) (collectively, the "Losses") suffered or incurred by any of them in connection with any claim, demand, suit or judgement involving any actual or alleged infringement of any patent, copyright, trademark or other intellectual property rights ("Intellectual Property Rights") in connection with the manufacture, use or disposition of any goods, article, material or service supplied by Seller. Seller will, at its expense, defend all claims, actions or proceedings against Buyer relating to or based on any allegation that the services, or any part of the services, constitutes an infringement upon, or a misappropriation of any Intellectual Property Rights and will pay to Buyer all resulting Losses incurred by Buyer. Buyer will give Seller written notice of any such claim, action or proceeding and, at the request and expense of Seller, provide all available information, assistance and authority required to conduct its defence. If all or any part of the services is finally determined to constitute an infringement or misappropriation of Intellectual Property Rights of a third party, or if Buyer is enjoined from using any of the services or Intellectual Property Rights embodied therein as a result of an infringement or misappropriation claim, Seller will at its expense promptly: (i) obtain for Buyer the right to continue using the services; (ii) replace the infringing elements of the services with non-infringing elements, while maintaining the full functionality, integrity and performance capabilities of the services; or (iii) modify the services so that it no longer infringes, while maintaining the full functionality, integrity and performance capabilities of the services.

9. Indemnification. To the fullest extent permitted by law, Seller shall indemnify and hold harmless Indemnified Parties from and against any and all Losses suffered or incurred by any of them in connection with any actual or alleged damage to property or injury (including death) to any person arising from or in connection with the services provided by Seller or the use thereof, Seller's performance under this Order, or Seller's performance of work on Buyer's premises or use of Buyer's property, either on or off of Buyer's premises, except for such arising solely out of the gross negligence of Buyer.

10. Limitation of Liability. To the fullest extent permitted by law, Buyer shall not be liable to Seller, its employees, representatives, agents, suppliers, or subcontractors for any anticipated profits or incidental damages (except to the extent expressly provided in Section 12) or consequential damages. Without limiting the foregoing, Buyer's liability for any claim arising directly or indirectly under or in connection with the Order shall in no event exceed the cost of the services giving rise to the claim. Buyer shall have no liability for penalties of any kind.

11. Laws and Regulations. Seller shall comply with all applicable laws (including federal, provincial and municipal statutes, regulations and bylaws) of whatever nature concerning the performance of the services. Unless otherwise specified in this Order Seller will obtain, at its cost, all permits and other consents required in respect of the services.

Seller shall also, at its sole expense, obtain an A, B, or C grade in ISNetworld as determined by Buyer based on the type of work being performed prior to the commencement of the Work. Seller shall maintain such grade in ISNetworld or shall obtain a documented variance to such grade requirement from Buyer for the term. Once obtained, if at any time Seller's ISNetworld grade falls below the requisite grade, Seller shall have thirty (30) days to re-attain such grade. Failure to maintain such grade may result in probationary action being taken against Seller or in the termination of the Agreement without penalty to Buyer.

Notwithstanding the above-noted paragraph, Buyer may, in its sole and absolute discretion, temporarily waive the requirement for an ISNetworld grade status if there is an urgent operational need to do so and Buyer is satisfied that Seller is working diligently toward obtaining the requisite ISNetworld grade.

12. Termination for Convenience. Buyer may, by written notice to Seller, terminate the Order, or any part thereof, for any or no reason, for Buyer's convenience. Upon notice of termination, Seller shall immediately stop all work and cause its suppliers and/or subcontractors to stop all work in connection with the Order. If Buyer terminates for convenience, Buyer shall pay Seller for services accepted as of the date of termination, and, subject to Section 10, for Seller's actual, reasonable, out of pocket costs incurred directly as a result of such termination. Buyer shall have no responsibility for work performed after Seller's receipt of notice of termination.

13. Termination for Cause. Buyer may, by written notice to Seller, terminate the Order, or any part thereof, if Seller breaches any of the terms and conditions of the Order, becomes insolvent or is declared bankrupt. By way of example, (a) failure by Seller to make timely, complete and conforming delivery of services, or (b) breach of the representations or warranties set forth in the Order, shall entitle Buyer to terminate the Order for cause. If Buyer terminates for cause, Buyer shall have no payment obligations to Seller. Should a court of competent jurisdiction subsequently determine that Buyer's termination for cause was wrongful or unjustified, then such termination shall be automatically considered a termination for convenience under Section 12 and Seller shall have all rights under that provision, but no other rights or claims for damages.

14. Confidentiality. Seller acknowledges that it may, in providing the performance of its services under the Order, be exposed to or acquire proprietary confidential information of Buyer or any of its affiliates, including, without limitation, information or materials concerning any of Buyer's or any such affiliate's customers, organization, work, know-how, processes, manufacturing techniques or technology ("Confidential Information"). Seller agrees to hold the Confidential Information in strict confidence and not to copy, reproduce, sell, assign, license, market, transfer, or otherwise disclose to any person or entity any such Confidential Information or to use any of such Confidential Information for any purpose other than in the performance of Seller's obligations under this Order. Seller agrees to notify its agents, employees and subcontractors of this confidentiality requirement and to obligate them in writing to abide by it for the express benefit of Buyer and its affiliates.

15. Use of Buyer's Name. Seller shall hold the business relationship with the Buyer and any Buyer's affiliate in strict confidence and shall not publish any advertising, promotion or other printed material or show any presentations or participate in any other activity which would disclose that it had or has a business relationship with Buyer or its affiliates and/or any details of that relationship.

16. Survival; Remedies Cumulative. All agreements, representations and warranties of Seller herein (including without limitation those regarding confidentiality and indemnification) shall survive delivery and final payment or an earlier termination of any Order. All of the rights and remedies available to Buyer under any Order are in addition to, and not in limitation of, the rights and remedies otherwise available at law or in equity.

17. Governing Law. This Order and the conduct of the parties with respect to the formation and performance of this Order are governed by and are to be construed and interpreted in accordance with the laws of Ontario and the laws of Canada applicable in Ontario. The parties irrevocably submit to the non-exclusive jurisdiction of the Courts of Ontario and the Federal Court of Canada.

18. Miscellaneous. The invalidity, illegality or unenforceability of any provisions of any Order shall not affect the continuation in force of the remainder of said Order. No waiver of any obligation of Seller shall be effective unless in writing signed by Buyer and no waiver in any single instance shall be considered a waiver of any other or similar obligation. Any Order shall inure to the benefit of Buyer and its successors and assigns, shall be binding upon Seller and its successors and assigns and may not be assigned or delegated by Seller without the express written consent of Buyer.

19. Dispute Resolution. All disputes, disagreements, controversies, questions or claims arising out of or relating to this Order, or in respect of any legal relationship associated with or arising from this Order, including with respect to this Order's formation, execution, validity, application, interpretation, performance, breach, termination or enforcement, will be determined by litigation in the Superior Court of Justice of Ontario at Ottawa, to the jurisdiction of which the parties irrevocably attorn.

20. Seller acknowledges and agrees that in addition to the obligations set out herein, it shall comply with Buyer's privacy, artificial intelligence (AI) and security provisions set forth in Schedule "A" attached hereto.

Schedule "A" – Privacy, AI and Security

Definitions

"**AI Incident**" means an occurrence involving an AI System that results in or could result in unauthorized use, disruption, modification, or destruction of Client Data, including but not limited to: data poisoning, model confabulation or hallucination, adversarial attacks, material model bias or discrimination, model exploitation, or any other significant malfunction or misuse of an AI System that could impact reliability, integrity, safety, or security of Client Infrastructure or services.

"**Artificial Intelligence System**" or "**AI System**" means a technological system that, autonomously or partly autonomously, processes data or information using computational models to generate outputs such as predictions, recommendations, decisions, or other outcomes that influence environments, behaviors, or data, and includes systems that utilize machine learning, neural networks, large language models, or generative AI.

"**Asset**" means a device issued by the Contractor that possesses all industry-leading controls mechanisms.

"**Client Data**" means all electronic data or information provided by Client to the Contractor, including Personal Information and Confidential Information, in connection with the Work.

"**Client Infrastructure**" means all applications, networking, servers and Work that reside within Client's data centres and domains.

"**Handle**" means to access, receive, collect, use, transmit, store, process, record, disclose, transfer, retain, dispose of, destroy, manage or otherwise handle; and "Handling" has a corresponding meaning.

"**High-Risk AI System**" means an AI System that (i) is intended to be used in a manner that poses a significant risk to health, safety, fundamental rights, or critical infrastructure; (ii) is identified as high-risk under applicable laws or regulations; or (iii) meets the criteria for high-risk applications under the NIST AI Risk Management Framework or NIST Generative AI Profile.

"**Personal Information**" means information about an identifiable individual including, without limitation, his or her gender, marital status, address, telephone number, email addresses, financial information, bank information, electricity consumption and identifying numbers such as account numbers, to which Contractor is given access by Client for the purposes of this Agreement, and/or which is compiled by and stored using the Work, including all such information that is Client's Confidential Information, data and any information derived from such Personal Information including aggregate and de-identified information.

"**Privacy Breach**" means any action or inaction by Contractor that results, or may result, in: (i) the Handling of Client Data by any person who is not authorized or entitled to Handle such Client Data; or (ii) the loss of, or inability to account for, Client Data.

"**Security Breach**" means any breach of any provisions of the Agreement that Client determines, in its sole discretion, has caused or may cause unauthorized Handling of, or the loss of or inability to account for, Client Data (including a Privacy Breach).

"**Security Incident**" means:

i. violation or imminent threat of violation of Contractor's or Client's computer security policies, acceptable use policies, or standard security practices necessary for Contractor to provide the Work and perform its obligations under the Agreement;
ii. unauthorized delivery of, access to or use of Client Data, facilities, infrastructure, premises, computer systems, and/or hardware occurring by or through Contractor or its authorized personnel, whether intentional or otherwise;
iii. any act or omission of Contractor or its authorized personnel that compromises; (a) the security, confidentiality or integrity of Client Data, or (b) any physical, technical or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality or integrity of Client Data;
iv. potential, imminent or actual Security Breaches;
v. potential, imminent or actual Privacy Breaches;
vi. receipt of a complaint or allegation in relation to the privacy and security practices of Contractor or its authorized personnel; and
vii. breach or alleged breach of the Agreement relating to such Contractor privacy and security practices.

For clarity, an AI Incident shall be deemed to be a Security Incident for the purposes of this Agreement.

Privacy and Security

1. Contractor shall comply with all laws or regulations related to information security, privacy and data protection that are applicable to both Client and Contractor and shall employ industry-appropriate standards, including current best practices and frameworks, to safeguard, prevent, detect, identify, report, track and respond to Security Incidents. Contractor shall maintain documentation of its compliance with such standards and frameworks.

2. Contractor shall, where applicable: (a) monitor the Work for unauthorized access, interception, interruption, and Client Data loss using industry-appropriate network-based intrusion detection and prevention mechanisms and data loss prevention tools; (b) hold and safeguard Client Data in a secure physical and electronic environment using best practices: (i) that are not less rigorous than those used in the information technology services industry, (ii) that align with recognized security frameworks such as ISO 27001, SOC 2, or NIST CSF, and (iii) that a reasonable prudent and diligent commercial entity would undertake in similar circumstances (c) have plans and systems in place to isolate portions of the Work, software, hardware and/or infrastructure that Client provides Contractor with access to perform the Work and other obligations under this Agreement and any work order to ensure that if a portion of the Work, hardware, software and/or infrastructure fail due to the actions of Contractor, Contractor's authorized personnel and/or Contractor's subcontractors, or due to an intrusion or attack by a third party, that the remainder of Client's system, hardware, software and infrastructure will not be compromised and (d) comply with Client's cybersecurity policies.

3. Contractor shall, where applicable, ensure that any work performed on Client Infrastructure is done in an industry-appropriate, secure, remote access manner defined by Client within an approved Asset. Any software that is required by the Contractor to perform the Work

must be properly validated by Contractor to ensure it's malware-free and authentic prior to it being deployed on Client Infrastructure. Contractor must ensure that the mechanism through which any Client Data is to be extracted from Client Infrastructure is communicated with Client prior to such extraction to minimize any associated risk of Client Data loss or exposure. All Work must occur within Client's "Geo Fence" which is subject to change based on Client's current risk threshold. The "Geo Fence" defines what countries are permitted to access Client's infrastructure, a copy of which may be provided to the Contractor upon request.

4. Contractor will immediately, but no later than twenty-four (24) hours after becoming aware of any actual or reasonably suspected Security Incident, notify Client at cybersecurity@hydroottawa.com with copies to generalcounsel@hydroottawa.com and to Client's primary business contact with Contractor. Such notification shall include preliminary details about the nature and scope of the incident, the data potentially affected, and initial containment measures implemented. Immediately following Contractor's notification to Client of any actual or reasonably suspected Security Incident and upon Client's request, Contractor shall at its own expense coordinate with Client to investigate the incident. Contractor agrees to fully cooperate with Client in the Handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing Client with physical access to the facilities and operations affected; (iii) facilitating interviews with employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry-leading standards or as otherwise reasonably required by Client.

5. At any time during the term of this Agreement and upon Client's reasonable request, Contractor will provide to Client a copy of Contractor's security documentation which Contractor makes generally available to its customers, including reasonably available third party security audits or reviews and any written notice and detail of any deficiencies that Contractor's auditors (whether internal or external) found through the conduct of such audits, and the remediation efforts conducted by Contractor to rectify such deficiencies. Contractor may update or modify its security measures from time to time provided that: i) such updates and/or modifications do not result in the degradation of the security of the Work; and ii) Contractor notifies Client in writing of such updates and modifications immediately, but not later than twenty-four (24) hours from the date of such updates and/or modifications.

6. Upon Client's written request, Contractor shall within ten (10) Business Days of such request provide to Client an officer's certificate signed by a Contractor senior executive confirming and certifying the current Contractor security measures that are in place to safeguard, prevent, detect, identify, report, track and respond to Security Incidents. This certification shall specifically address compliance with all security requirements in this Agreement, including those related to data protection, encryption, access controls, and incident response procedures.

7. The Client shall have the right to conduct an annual audit of the Contractor's privacy and security practices. This audit may be independently satisfied by a third-party audit or assessment, conducted by an independent and objective auditor or assessor, that complies with a recognized standard such as NIST. In the event that a security incident or privacy breach occurs, the Client retains the right to conduct its own audit of the Contractor's privacy and security practices, notwithstanding any third-party audits. This clause is separate and independent from the Client's rights to audit AI Systems as specified in the subsequent section.

Artificial Intelligence Systems

8. Contractor shall not use any AI System to process Personal Information or in providing services that may impact reliability or infrastructure without prior written disclosure to and approval from Client. Any use of an AI System without such disclosure and approval shall constitute a material breach of this Agreement.

9. Where Contractor uses or intends to use an AI System in connection with the Work, Contractor shall provide to Client, prior to processing Personal Information or providing any services that may impact reliability or infrastructure, detailed written disclosures including:
    a. identification of the specific AI System(s) being used;
    b. purposes for which the AI System is being used;
    c. types of data processed by the AI System;
    d. dependencies on the AI System for service delivery;
    e. potential risks associated with the AI System;
    f. whether the AI System is considered high-risk under applicable laws or regulations or NIST guidelines; and
    g. technical and organizational measures implemented to mitigate risks.

10. Contractor shall comply with all obligations under the *Enhancing Digital Security and Trust Act, 2024 (Bill 194)*, the *Freedom of Information and Protection of Privacy Act (FIPPA)*, and the cybersecurity requirements under Bill C-8, including:
    a. supporting Client's regulatory reporting requirements;
    b. providing periodic formal reporting on AI System use;
    c. maintaining records of AI System development, training, and operation; and
    d. cooperating with Client's compliance activities, including Privacy Impact Assessments and AI accountability frameworks required under applicable laws.

11. Contractor shall support data subject rights by:
    a. facilitating access, correction, and deletion requests related to Personal Information processed by AI Systems;
    b. providing transparency regarding AI System logic and impacts;
    c. implementing additional safeguards for High-Risk AI Systems, including explainability measures and enhanced oversight; and
    d. maintaining documentation sufficient to respond to inquiries from data subjects or regulators.

12. In addition to the Security Incident notification obligations set forth in this Schedule, Contractor shall:
    a. immediately notify Client of any AI Incident;
    b. implement immediate containment and remediation measures for AI Incidents;
    c. provide Client with all information necessary to understand the nature, cause, and impact of the AI Incident; and
    d. cooperate with Client in investigating and remediating the AI Incident, including suspending use of the AI System if requested by Client.

13. Contractor shall implement and maintain AI governance and risk management practices aligned with the NIST AI Risk Management Framework (AI RMF) and NIST Generative AI Profile, including:
    a. conducting and documenting AI risk assessments;
    b. implementing continuous monitoring of AI System performance;
    c. maintaining appropriate safeguards commensurate with identified risks; and
    d. adapting controls as new risks are identified or as AI capabilities evolve.

14. Contractor shall implement and maintain a "kill-switch" or suspension functionality for all AI Systems used in connection with the Work, which shall:
    a. allow for immediate pausing or termination of AI System operation;
    b. be activated upon Client's request at Client's sole discretion;
    c. be activated automatically in the event of detection of significant anomalies or AI Incidents; and
    d. be tested periodically to ensure proper functioning.

15. Client shall have the right to review and audit Contractor's AI Systems, including:
    a. information on how data is used to train or operate AI Systems;
    b. reviewing AI models, algorithms, and control mechanisms;
    c. assessing compliance with this Schedule and applicable laws and regulations; and
    d. accessing documentation of AI System development, testing, and risk assessments.

    Contractor shall cooperate fully with such audits and provide all information and access reasonably requested by Client, subject to appropriate confidentiality safeguards and data protection measures during the audit process.

16. Contractor shall exercise ongoing diligence regarding AI Systems by:
    a. providing timely updates to Client regarding changes to AI usage, risks, privacy impacts, and security vulnerabilities;
    b. monitoring for and promptly addressing any bias, discrimination, privacy violations, security vulnerabilities, or other harmful outputs;
    c. maintaining appropriate documentation of AI System performance, incidents, and compliance activities; and
    d. updating safeguards as needed to address emerging risks or regulatory requirements.

Liability

In the event that Contractor breaches any obligations set forth in this schedule related to security, privacy, or AI, Contractor shall be liable to Client for any direct damages arising from such breach. Contractor shall notify Client immediately upon becoming aware of any such breach, providing all relevant details including the nature of the breach, data affected, and measures taken to contain and remediate the situation. Contractor agrees to indemnify and hold harmless Client from any claims, losses, or damages arising out of or in connection with such breach, subject to the limitations of liability set forth in the Agreement. Contractor shall also bear all costs associated with the notification of affected individuals and any regulatory bodies as required by applicable law. Furthermore, Contractor shall cooperate fully with Client in investigating and resolving the breach, including providing all necessary access and information as requested by Client. This clause does not limit any other rights or remedies available to Client under this Agreement or applicable law.