Cyber Application

Intended for our clients generating less than $250M revenues annually.

Network Security and Privacy Liability

Client name:

Is the applicant the parent entity? ☐ Yes ☐ No

If no, please supply details:

Street address:

City: **Prov.:** **Postal code:**

Web address: **Client industry:**

Client contact: **Contact email:**

Revenues (CAD): **Last fully completed year:** $ **Projected annual figure:** $

No. of employees:

1. **Do you currently have cyber coverage in place?** ☐ Yes ☐ No
2. **Please advise approximate number of unique personally identifiable information (PII) records stored on your network, database or system (including those stored on your behalf of third-party networks):** Unknown
3. **If available, please advise exact number of unique PII records stored:**
4. **Do you collect personal health information (PHI) from your customers (excluding employees)?** ☐ Yes ☐ No
   If yes, please advise approximate number of unique PHI records stored on your network, database or system (including those stored on your behalf of third-party networks): Unknown
5. **If available, please advise exact number of unique PHI records stored:**
6. **Do you collect credit card information?** ☐ Yes ☐ No
   If yes, please advise the number of credit card records stored: Unknown
7. **Are you Payment Card Industry (PCI) compliant?** ☐ Yes ☐ No
8. **Are you involved in the direct supply of goods or services to the cannabis industry?** ☐ Yes ☐ No
9. **Are you involved directly with the use or supply of cryptocurrency?** ☐ Yes ☐ No

AON

10. **Is your operational technology (OT) environment segmented from both your Information Technology (IT) environment and the internet (if applicable)?** ☐ N/A ☐ Yes ☐ No

Email Security

11. **Do you pre-screen emails for potentially malicious attachments and links?** ☐ Yes ☐ No

12. **Do you conduct phishing training on an annual basis?** ☐ Yes ☐ No

13. **Are employees required to complete security training on at least an annual basis?** ☐ Yes ☐ No

14. **Do you require dual control when transferring funds in excess of CAD 25,000?** (Dual control refers to a process by which a transfer must be approved or confirmed by someone other than the initiator of the transfer.) ☐ Yes ☐ No

Multi-factor Authentication

15. **Is multi-factor authentication (MFA) required for access to privileged user accounts?** ☐ Yes ☐ No

16. **Do you enforce MFA for all users, including third parties and those connecting remotely to the network?** ☐ Yes ☐ No

17. **Do you enforce MFA for all email access?** ☐ Yes ☐ No

Encryption, Endpoint Protection, Patches, and Backups

18. **Do you have access control procedures and hard drive encryption to prevent unauthorized access on your databases, servers, and data files?** ☐ Yes ☐ No

19. **Do you use a paid for endpoint protection (EPP) product across your enterprise?** ☐ Yes ☐ No

    Do you use any other security solutions to prevent or detect malicious activity on your network (options include the following: Endpoint Detention and Response (EDR), Managed Detection and Response (MDR), or Network Detection and Response (NDR)? ☐ Yes ☐ No

20. **Do you install critical and high severity patches across your enterprise within one month?** ☐ Yes ☐ No

21. **Do you have procedures to back up, archive, and restore sensitive data and critical business systems?** ☐ Yes ☐ No

22. **Are your backups kept separate from your network ("offline"), in a cloud service designed for this purpose, or stored on a separate device or service which cannot be accessed from your network?** ☐ Yes ☐ No

23. **How often are your backups performed?** Other (please specify below)

24. **Have you tested the successful restoration and recovery of key server configurations and data from backups in the last six months?** ☐ Yes ☐ No

Media and Miscellaneous

25. **Within the last three years, has the client been subject to any complaint concerning the content of its website, advertising materials, social media or other publications?** ☐ Yes ☐ No

26. **Do you have procedures in place to review media content prior to release on your website?** ☐ Yes ☐ No

27. **Does the client have procedures to remove content (including third-party content) that is libelous, infringing, or otherwise controversial?** ☐ Yes ☐ No

Loss History

28. **Has the insured had any prior cyber-related claims or incidents in the last five years?** ☐ Yes ☐ No

29. **Has the insured had any prior cyber-related claims where outside vendors were used for remediation?** ☐ Yes ☐ No

30. **Has the insured had any prior cyber-related claims where the costs incurred would have been above the retention of the cyber policy?** ☐ Yes ☐ No

31. **Has the insured had any legal action brought or threatened against them in the last five years as a direct result of a cyber event?** ☐ Yes ☐ No

If yes to any of the questions above, please provide details on the loss including the cost incurred and post-loss improvements that were implemented. Disclaimer: do not include items fixed in-house without cost.

Please provide any additional commentary on your risk posture:

This application must be signed and dated by a member of the control group. Control group means any principal, partner, corporate officer, director, member, general counsel (or most senior legal counsel) or risk manager of the insured organization, and any individual in a substantially similar position.

Signature: _____ **Date:** _____

Disclaimer: By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. Aon will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data.

Privacy Notice

The collection, use and disclosure of personal information through this site and Aon's services is governed by Aon's Privacy Policy http://www.aon.com/canada/about-aon/privacy.jsp.

Highlights

Aon collects, uses and discloses personal information:

- To determine eligibility and process applications for products and services and to provide information and services
- To understand and assess ongoing needs of clients and potential clients and offer products and services to meet those needs
- For communication, service, marketing, billing and administration
- For claims administration and data analysis
- For fraud detection and prevention
- For analytics purposes by aggregating or otherwise de-identifying personal information
- To develop proprietary tools and databases
- To provide consulting services to insurance companies
- To comply with legal, audit, security and regulatory requirements
- To obtain and update credit information with appropriate third parties, such as credit reporting agencies, where transactions are made on credit
- Other purposes disclosed in our Privacy Policy or our terms of business or disclosed to you at the time of collection, use or disclosure

Each Applicant authorizes Aon to collect and/or disclose the Applicant's personal information from/to third parties such as insurance companies, other brokers, adjusters, agencies, motor vehicle/driver licensing authorities and others as may be required for the above purposes. If the Applicant is providing any additional insured personal information, the Applicant providing this information warrants having obtained the prior written consent from each additional insured for the collection, use and disclosure of their personal information as set out herein.

Aon uses affiliates and/or third service providers. These affiliates and service providers may operate outside of Canada and, therefore, your personal information may be subject to the laws of other jurisdictions.

For further information, including how to contact Aon's Privacy Officer, please read Aon's Privacy Policy available at http://www.aon.com/canada/about-aon/privacy.jsp.