Phone 1 877 814 7778

submissions.canada@beazley.com
renewals.canada@beazley.com
info.canada@beazley.com
www.beazley.ca

Beazley Canada Limited

First Canadian Place
100 King Street West
Suite 4530, P.O. Box 328
Toronto, Ontario M5X 1E1

Phone (416) 601 2155
Fax (416) 861 1617

310-1130 Sherbrooke Street West
Montreal, Quebec H3A 2M8

Phone (514) 350 4848
Fax (514) 350 0843

906-1021 West Hastings Street
Vancouver, British Columbia V6E 0C3

Phone (778) 373 4432

BEAZLEY BREACH RESPONSE INSURANCE APPLICATION (BBR)

INFORMATION SECURITY & PRIVACY INSURANCE WITH BREACH RESPONSE SERVICES

THIS APPLICATION IS FOR A CLAIMS MADE AND REPORTED POLICY:

1. GENERAL INFORMATION

1. Name of Organization or Legal Entity (Applicant) including any subsidiaries:

   (please show complete name as you wish it to appear on the policy)

2. Address (Not P.O. Box):

3. Number of Employees: _____

4. Website(s): _____

5. The Company is Canadian registered? ☐ YES ☐ NO

6.

Authorized Officer 1:	Email:	Telephone:
Breach Response Contact 2:	Email:	Telephone:

2. COMPANY INFORMATION

7. Please provide a brief description of your business:

REVENUE INFORMATION

8. **FOR ALL APPLICANTS, PLEASE PROVIDE GROSS REVENUE INFORMATION**

	MOST RECENT TWELVE (12) MONTHS	NEXT YEAR (Estimate)
CDN Revenue:		
USD Revenue:		
OTHER Revenue (specify)		
TOTAL:		

9. What percentage of the Applicant's revenues is business to business? _____% Direct to consumer _____%

10. Are significant changes to the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months? ☐ YES ☐ NO
    If YES, please explain:

11. Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? ☐ YES ☐ NO
    If YES, please explain:

[1] This is the officer of the Applicant that is authorized to make statements to the Underwriters on the Applicant's behalf and to receive notices from the Insurer or its authorized representative(s).
[2] This is the employee of the Applicant that is designated to work with the insurer in response to a data breach event.

3. PRIVACY

12. Does the Applicant collect, process, or maintain private or personal information as part of its business activities? ☐ YES ☐ NO
If YES:
a) Identify which Personal Identifiable Information (PII) is being held:

Social Security Numbers	☐	Bank Account Information	☐
Credit Card Information	☐	Individual Names and Addresses	☐
Employee Information	☐	Email Addresses	☐
Personal Health Data	☐	Third Party Corporate Information	☐
Other (Specify):	☐		

b) Provide the number of records maintained by the Applicant containing the above information (approx.):
☐ 0 – 20,000 ☐ 20,000 – 50,000 ☐ 50,000 – 100,000 ☐ 100,000 – 200,000 ☐ > 200,000**
** If number is greater than 200,000 enter estimated number of PII records maintained here):_____

13. Has the Applicant designated a Chief Privacy Officer? ☐ YES ☐ NO
If No: please indicate what position (s) (if any) are responsible for privacy issues:_____

14. Does the Applicant require third parties with which it shares personally identifiable or confidential information to indemnify the Applicant for Legal Liability arising out of the release of such information due to the fault of negligence of the third party? ☐ YES ☐ NO

3. PAYMENT CARDS

15. Does the Applicant accept credit cards for goods sold or services rendered? ☐ YES ☐ NO
If YES, is the Applicant compliant with applicable data security standards e.g., Payment Card Industry (PCI) Data Security Standard (DSS)? ☐ YES ☐ NO

a) Please state the Applicant's approximate percentage of revenue from credit card transactions in the most recent twelve (12) months:
_____%

16. If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:_____

17. Is payment card data encrypted at the point of sale (e.g. payment card reader or e-commerce payment portal) through transmission to the payment processor? ☐ YES ☐ NO

4. COMPUTER SYSTEMS CONTROL

18. Has the Applicant designated a Chief Security Officer in regards to computer systems? ☐ YES ☐ NO
If NO, please indicate what position is responsible for computer security:

19. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? ☐ YES ☐ NO

20. Does the Applicant conduct computer and information security training for all employees, including owners, that have access to computer systems or sensitive data at least on an annual basis? ☐ YES ☐ NO

21. Confirmation that the Applicant implements critical patches and updates systems as soon as possible when updates and patches become available, and do not use any end-of-life/unsupported software. ☐ YES ☐ NO

22. Confirmation that the Applicant uses MFA (Multi-factor Authentication) for accessing email through a website or cloud base service and for all remote access to the network. ☐ YES ☐ NO

23. Confirmation that the Applicant does not allow remote access into the environment without a VPN (Virtual Private Network). ☐ YES ☐ NO

24. Confirmation that the Applicant scans incoming emails for malicious attachments and/or links. ☐ YES ☐ NO

25. Confirmation that the Applicant protects all of devices with anti-virus, anti-malware, and/or endpoint protection software. ☐ YES ☐ NO

26. Does the Applicant restrict user rights on computer systems such that individuals (including third party service providers) have access only to those areas of the network or information that is necessary for them to perform their duties? ☐ YES ☐ NO

27. Where does the Applicant have a firewall? (Check all that apply).
☐ At network perimeter ☐ internally within the network to protect sensitive resources

28. Which of the following procedures does the Applicant employ to test computer security controls?

Testing	Frequency of testing		
☐ Internal Vulnerability Scanning	☐ Continuously	☐ Monthly	☐ Quarterly
☐ External Vulnerability Scanning against Internet-facing IP Addresses	☐ Continuously	☐ Monthly	☐ Quarterly
☐ Penetration Testing	☐ Continuously	☐ Semi-annually	☐ Quarterly

☐ Other (Please describe):
_____

29. Does the Applicant have network intrusion detection systems that provide actionable alerts if an unauthorized computer system intrusion occurs? ☐ YES ☐ NO

30. Does the Applicant store data in any of the following environments, and is such stored data encrypted? (check all that apply).

☐ Laptops	☐ Encrypted	☐ Not Encrypted
☐ Portable Media	☐ Encrypted	☐ Not Encrypted
☐ Back-up Tapes	☐ Encrypted	☐ Not Encrypted
☐ "at rest" written computer databases	☐ Encrypted	☐ Not Encrypted
☐ While in transit	☐ Encrypted	☐ Not Encrypted

31. Does the Applicant outsource any of the following? (Check all that apply and please identify the vendor(s).
☐ Data Center Hosting: _____
☐ Managed Security: _____
☐ Alert Log Monitoring: _____

5. BUSINESS CONTINUITY

32. Does the Applicant have:
a) A disaster recovery plan? ☐ YES ☐ NO Date last tested: _____
b) A business continuity plan? ☐ YES ☐ NO Date last tested: _____
c) An incident response plan for network and virus incidents? ☐ YES ☐ NO Date last tested: _____

33. If the Applicant has a business continuity plan, does the plan contain recovery time objectives for the amount of time within which business processes and continuity must be restored? ☐ YES ☐ NO

34. Details regarding back up procedures:

Backups performed, at minimum, on daily basis	☐ YES ☐ NO
Backups are stored in a segregated or non-networked environment	☐ YES ☐ NO
Backups are encrypted	☐ YES ☐ NO
Integrity of backups are tested regularly to ensure they are recoverable	☐ YES ☐ NO

If NO to any of the above, please provide explanation.

6. MEDIA LIABILITY

35. Please describe the media activities of the Applicant or by others on behalf of the Applicant:
☐ Television ☐ Radio
☐ Print ☐ Applicant's Website (s)
☐ Internet Advertising ☐ Social Media
☐ Marketing Materials ☐ Audio or Video Streaming

36. Does the Applicant have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to any publication, broadcast, distribution or use? ☐ YES ☐ NO

37. Does the Applicant have a process to review all content prior to posting on the Insured's website or on social media web pages created and maintained by or on behalf of the Insured? ☐ YES ☐ NO
If YES, is the review performed by a qualified attorney? ☐ YES ☐ NO

38. Does the Applicant allow user generated content to be displaced on its website(s)? ☐ YES ☐ NO

7. E-CRIME

39. Are all employees that are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering (fraudulent instructions) , phishing, business email compromises and other scams on at least an annual basis. ☐ YES ☐ NO

40. Before processing fund transfer requests from internal sources, does the Applicant confirm the instructions via a method other than the original means of the instruction? ☐ YES ☐ NO

41. Do the Applicant's procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions? ☐ YES ☐ NO

42. When a vendor/supplier requests any change to its account details (including routing numbers, account numbers, telephone numbers and contact information) and prior to making any changes:
    a) Does the Applicant first confirm all changes requested by the vendor/supplier with a person other than the requestor prior to making any changes? ☐ YES ☐ NO
    b) Does the Applicant confirm requested changes via a method other than the original means of request? ☐ YES ☐ NO

43. Do the Applicant's processes and procedures require review of all requests by a supervisor or next-level approver? ☐ YES ☐ NO

8. PRIOR CLAIMS AND CIRCUMSTANCES

44. Does the Applicant or other proposed insured, or any director, officer or employee of the Applicant or other proposed insured have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim or loss or obligation to provide breach notification under the proposed insurance? ☐ YES ☐ NO

    If YES, please provide details:

45. During the last five (5) years, has the Applicant:

    1) Received any claims or complaints with respect to privacy, breach of information or network security, unauthorized disclosure of information or defamation or content infringement? ☐ YES ☐ NO

    2) Been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation? ☐ YES ☐ NO

    3) Notified consumers or any other third party of a data breach incident involving the Applicant? ☐ YES ☐ NO

    4) Experienced an actual or attempted extortion demand with respect to its computer systems? ☐ YES ☐ NO

    If YES, please provide details of any such action, notification, investigation or subpoena:

Without limitation of any other remedy available to the Insurer, it is hereby agreed that if there be knowledge of any of the matters described above, any written demand or civil proceedings for compensatory damages subsequently emanating therefrom is excluded from coverage under the proposed insurance.

NOTICE CONCERNING PERSONAL INFORMATION

By purchasing insurance from Beazley Canada Limited, a customer provides Beazley with his or her consent to the collection, use and disclosure of personal information, including that previously collected, for the following purposes:

- the communication with underwriters;
- the underwriting of policies;
- the evaluation of claims;
- the detection and prevention of fraud;
- the analysis of business results;
- purposes required or authorized by law.

For the purposes identified above, personal information may be disclosed to Beazley's related or affiliated companies and service providers.

Further information about Beazley's personal information protection policy may be obtained by contacting their privacy officer at 416-601-2155.

WARRANTY STATEMENT

The undersigned warrants that to the best of their knowledge, the statements set forth in this Application are true. The undersigned also warrants that they have not suppressed or misstated any material fact.

If the information provided in this Application should change between the date of the Application and the effective date of the policy, the undersigned warrants that they will immediately report such changes to the Insurer.

Signing this Application does not bind the undersigned to purchase this insurance, nor does it bind the Insurer to issue this insurance. However, should the Insurer issue a policy, this Application shall serve as the basis of such policy and will be attached to and form part thereof.

SIGNED:_____ DATE:_____
(Authorized Representative)

NAME (Please Print):_____ TITLE/POSITION: _____