Phone 1 877 814 7778

submissions.canada@beazley.com
renewals.canada@beazley.com

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

Beazley Canada Limited

550-55 University Avenue
Toronto, Ontario M5J 2H7

Phone (416) 601 2155
Fax (416) 601 2166

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

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

1511-701 West Georgia Street
Vancouver, British Columbia V7Y 1C6

Phone (778) 373 4432

BEAZLEY BREACH RESPONSE INSURANCE APPLICATION (BBR)

INFORMATION SECURITY & PRIVACY INSURANCE WITH BREACH RESPONSE SERVICES

NOTICE: INSURING AGREEMENTS A., C., D. AND E. OF THIS POLICY PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD OR AS OTHERWISE PROVIDED IN CLAUSE X. OF THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

INSURING AGREEMENT B. OF THIS POLICY PROVIDES FIRST PARTY COVERAGE ON AN INCIDENT DISCOVERED AND REPORTED BASIS AND APPLIES ONLY TO INCIDENTS FIRST DISCOVERED BY THE INSURED AND REPORTED TO THE UNDERWRITERS DURING THE POLICY PERIOD.

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: _____

5. The Applicant has continuously been in business since (Month/Year): _____

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

2. COMPANY INFORMATION

7. Please provide a brief description of your business:

_____

_____

8. Does the Applicant provide data processing, data storage, or data hosting services to third parties? ☐ YES ☐ NO
If YES, please comment on the specific service in the description above:

_____

_____

9. Does the Applicant distribute any products on a wholesale basis? ☐ YES ☐ NO
If YES, please confirm the percentage of revenue generated by wholesale distribution: _____

3. REVENUE INFORMATION

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

	MOST RECENT TWELVE (12) MONTHS (ending ____/____)	PREVIOUS YEAR	NEXT YEAR (Estimate)
CDN Revenue:			
USD Revenue:			
OTHER Revenue (specify) _____			
TOTAL:			

11. 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:

12. 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:

4. MANAGEMENT OF PRIVACY EXPOSURE

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

14. Does the Applicant have a written corporate-wide privacy policy? ☐ YES ☐ NO
If YES, please attach a copy of the privacy policy to this application.

15. Is the Applicant in compliance with its privacy policy? ☐ YES ☐ NO
If NO, please provide details regarding such non-compliance:

16. Does the Applicant collect, process, or maintain private or personal information as part of its business activities? ☐ YES ☐ NO
If YES:
1) 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):	☐	_____	

2) 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): _____

17. 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
1) Please state the Applicant's approximate percentage of revenue from credit card transactions in the most recent twelve (12) months: _____%

2) Is the Application compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? ☐ YES ☐ NO

3) 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:

18. Does the Applicant restrict employee access to personally identifiable information on a business-need to know basis? ☐ YES ☐ NO

19. Does the applicant require third parties with which it shares personally identifiable information or confidential information to idemnify the Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? ☐ YES ☐ NO

20. Has the Applicant implement an identity theft prevention program (aka FTC "Red Flags" program)? ☐ YES ☐ NO

21. If the Applicant is in the healthcare industry, does the Applicant host, operate or manage a Healthcare Information Exchange on which other organizations may store personal health information? ☐ YES ☐ NO

5. COMPUTER SYSTEMS CONTROL

22. 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:

_____

_____

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

24. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? ☐ YES ☐ NO

25. Does the Applicant have:
1) A disaster recovery plan? ☐ YES ☐ NO
2) A business continuity plan, recovery plan and/or incident response plan? ☐ YES ☐ NO
3) An incident response plan for network and virus incidents? ☐ YES ☐ NO
4) How often are such plans tested? _____

26. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis? ☐ YES ☐ NO
If YES, please summarize the scope of such audits and/or tests:

_____

_____

27. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? ☐ YES ☐ NO

28. Is all valuable/sensitive data backed-up by the Applicant on a daily basis? ☐ YES ☐ NO
If NO, please describe exceptions: _____

29. Is at least one complete back-up file generation stored and secured offsite separate from the Applicant's main operations in a restricted area? ☐ YES ☐ NO
If NO, please describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive date offsite?

_____

_____

30. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted? ☐ YES ☐ NO
a) Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives? ☐ YES ☐ NO
b) Does the Applicant encrypt data stored on laptop computers and portable media? ☐ YES ☐ NO
c) Please describe any additional controls the Applicant has implemented to protect data stored on portable devices:

_____

_____

31. What format does the Applicant utilize for backing up and storage of computer system data?
☐ Tape or other media ☐ Online backup service ☐ Other: _____

a) Are tapes or other portable media containing backup materials encrypted? ☐ YES ☐ NO
b) Are tapes or other portable media stored offsite using secured transportation and secured facilities? ☐ YES ☐ NO
1) If stored offsite, are transportation logs maintained? ☐ YES ☐ NO
2) If stored onsite, please describe physical security controls:

_____

_____

32. Does the Applicant enforce a software update process including installation of software "patches"? ☐ YES ☐ NO
If YES, are critical patches installed within thirty (30) days of release? ☐ YES ☐ NO

33. Please describe your network infrastructure:

	ANTI-VIRUS	FIREWALL	ISP	INTRUSION DETECTION
Primary Vendor:				
Other significant vendor:				

34. How often are virus signatures updates?
☐ Automatic Updates ☐ Weekly ☐ Monthly ☐ Other: _____

35. Does the Applicant require computer service providers who may have access to confidential information or personally identifiable information to demonstrate adequate security policies and procedures? ☐ YES ☐ NO
a) Are computer service providers required by contract to indemnify the Applicant for harm arising from a breach of the provider's security? ☐ YES ☐ NO

6. WEBSITE CONTENT CONTROLS

36. Please check all descriptions of website content posted by the Applicant, including content posted to social media web pages:
☐ No Website ☐ Information created by the Applicant
☐ Content under license from a third arty ☐ Streaming video or music content
☐ Unlicensed third party content (i.e. Blog/Message Board/Customer Reviews)

37. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Application is libelous, infringing or in violation of a third party's privacy rights? ☐ YES ☐ NO
If YES, please provide details: _____

38. Does the Applicant have a process to review all content prior to posting on the Insured's Internet Site 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

39. Does the review include screening the content for the following:
1) Disparagement issues? ☐ YES ☐ NO
2) Copywriting infringement? ☐ YES ☐ NO
3) Trademark infringement? ☐ YES ☐ NO
4) Invasion of privacy? ☐ YES ☐ NO
If the Applicant does not have a process to review all content prior to posting, please describe the procedures to avoid posting of improper or infringing content:

_____

_____

40. Has the Applicant screened all trademarks used by the Applicant for infringement with existing trademarks prior to first use? ☐ YES ☐ NO
a) Has the Applicant acquired any trademarks from others in the past three (3) years? ☐ YES ☐ NO
If YES, were acquired trademarks screened for infringement? ☐ YES ☐ NO

7. PRIOR INSURANCE

41. Does the applicant currently have insurance in place covering media, privacy or network security exposures? ☐ YES ☐ NO
If YES, please complete the following:
Insurer: _____ Policy Period: _____
Limit of Liability: _____ Deductible: _____
Premium: _____ Retroactive Date: _____

42. Has any professional liability, privacy, network security or media insurance ever been declined, non-renewed or cancelled? ☐ YES ☐ NO
If YES, please provide details:

_____

_____

8. PRIOR CLAIMS AND CIRCUMSTANCES

43. 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:

_____

_____

44. 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.

9. 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.

10. 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:** _____