



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. The Company is Canadian registered? YES NO
5. Authorized Officer¹: _____ Email: _____ Telephone: _____
¹This is the officer of the Applicant that is authorized make statements to the Underwriters on the Applicant's behalf and to receive notices from the Insurer or its authorized representative(s).
6. Breach Response Contact²: _____ Email: _____ Telephone: _____
²This is the employee of the Applicant that is designated to work with the insurer in response to a data breach

2. REVENUE INFORMATION

7. For ALL Applicants, please provide Gross Revenue Information

	MOST RECENT TWELVE (12) MONTHS (ending ___/___)	PREVIOUS YEAR	NEXT YEAR (Estimate)
CDN Revenue:			
USD Revenue:			
TOTAL:			

3. PRIVACY

8. 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 <input type="checkbox"/>	Bank Account Information <input type="checkbox"/>
Credit Card Information <input type="checkbox"/>	Individual Names and Addresses <input type="checkbox"/>
Employee Information <input type="checkbox"/>	Email Addresses <input type="checkbox"/>
Personal Health Data <input type="checkbox"/>	Third Party Corporate Information <input type="checkbox"/>
Other (Specify): <input type="checkbox"/>	_____
9. 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): _____
10. 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

4. PAYMENT CARDS

11. Does the Applicant accept credit cards for goods sold or services rendered? YES NO
12. Is the Application compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? YES NO

5. COMPUTER SYSTEMS CONTROL

13. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? YES NO
14. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? YES NO
15. Does the Applicant have:
- a) A disaster recovery plan? YES NO
 - b) A business continuity plan, recovery plan and/or incident response plan? YES NO
 - c) An incident response plan for network and virus incidents? YES NO
 - d) How often are such plans tested? _____
16. Is all valuable/sensitive data backed-up by the Applicant on a daily basis? YES NO
Are backups performed daily? YES NO
Backups are stored in a segregated or non-networked environment. YES NO
Are backups encrypted? YES NO
Are backup integrity tested regularly YES NO
If NO to any of the above questions, please describe exceptions: _____
17. Does the applicant use the following controls?
- a) Commercially Available Firewall protection? YES NO
 - b) Commercially available anti-virus protection? YES NO
 - c) 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
 - d) Regular password and login updates? YES NO
18. Please confirm that MFA (Multi-factor Authentication - Two Factor Authentication) is being used for all remote access, including vendors. YES NO
If no, please provide explanation: _____

6. MEDIA LIABILITY

19. Does the applicant allow uncontrolled or unmonitored user generated content or posts on its website (i.e.) discussion group(s) forum(s), or electronic bulletin boards(s)? YES NO
20. 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: _____

7. E-CRIME

21. 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 bases. YES NO
22. 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
23. Do the Applicant's procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions? YES NO
24. 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: YES NO
25. 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

BEAZLEY BREACH RESPONSE (BBR)

26. Does the Applicant confirm requested changes via a method other than the original means of request? YES NO
27. 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

28. 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:

29. During the last five (5) years, has the Applicant:
- a) 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
- b) Been subject to any government action, investigation, or subpoena regarding any alleged violation of a privacy law or regulation? YES NO
- c) Notified consumers or any other third party of a data breach incident involving the Applicant? YES NO
- d) 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.

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: _____
(Authorized Representative)

DATE: _____

NAME (Please Print): _____

TITLE/POSITION: _____