



# Risk E-Business Cyber Loss And Liability Insurance Policy<sup>sm</sup>

**NOTICE: This application is for claims-made and reported coverage, which applies only to claims first made and reported in writing during the policy period or any extended reporting period. The limit of liability to pay damages or settlements will be reduced and may be exhausted by defense expenses and defense expenses will be applied against the deductible amount. The coverage afforded under this policy differs in some respects from that afforded under other policies. Read the entire application carefully before signing.**

1. Name \_\_\_\_\_  
 DBA \_\_\_\_\_  
 Name of Person Completing Application \_\_\_\_\_  
 Email Address \_\_\_\_\_

2. Type of Business (*select one*):  
 Private Corporation       Public Company       LLC  
 Partnership       Non-Profit       Investment Fund

3. Principal Address \_\_\_\_\_  
 City \_\_\_\_\_ Province \_\_\_\_\_ Postal Code \_\_\_\_\_  
 Primary Web Address \_\_\_\_\_

4. Please provide name, nature of operations, and relationship to the Company of all additional entities to be covered. Or, enter "none".

Additional Entity	Nature of Operations	Relationship to Company

Please complete each question for the remainder of this application with ALL entities above in mind (*herein after "the Company"*.)

## Background and Financial Information

5. Nature of business \_\_\_\_\_

6. Year Business Started \_\_\_\_\_

7. Total Number of Employees (*please include all full, part, time seasonal, leased, etc.*) \_\_\_\_\_

8. Please provide the following financial information:

Total Assets as of Most Recent Fiscal Year End	Total Gross Revenues Last Fiscal Year	Anticipated Revenues This Fiscal Year	Anticipated Revenues Next Fiscal Year
\$	\$	\$	\$

9. Percentage of Annual Revenues Estimated to be attributable to E-Commerce/Online Sales \_\_\_\_\_%

**Insurance Information****Yes No**

10. Has the Company experienced any of the following situations within the last three years?

Privacy Incident and/or claims?  Media Incident and/or claims?  Cyber Crime Incident?  Network Incident and/or claims?  

**If yes to any of the above**, please provide detail in a separate attachment a description of the incident including relevant dates, the number and type of records involved, the total dollar amount of expenses in connection with the incident, a summary of the Company's response to the incident, and subsequent changes made to prevent the likelihood of future events.

11. Do you presently purchase Cyber Risk Insurance?  **If yes**, please complete the following table.

Limits	Deductible	Continuity Date

12. Do you presently purchase Technology Errors and Omissions Insurance?  **If yes**, please provide the following:

Insurer	Limit	Deductible	Have you had any claims?
	\$	\$	<input type="checkbox"/> <input type="checkbox"/>

13. Are you aware of any fact, circumstance, or situation involving the Company that you have reason to believe will cause a Privacy Incident, Network Security Incident, Media Incident, Cyber Crime Incident, or Claim? (NOTE: Current Great American policyholders need not respond to this question)  

**It is understood and agreed that if you responded yes to the question above**, there is no coverage for any Privacy Incident, Network Security Incident, Media Incident, Cyber Crime Incident, or Claim based upon, arising out of, or in any way involving any such fact or circumstance.

**Social Engineering**

14. Indicate which of the following controls you have implemented with respect to electronic funds transfers:

 Callback procedures to verify funds transfer requests or changes to banking information Dual authorization for funds transfers greater than \$2,500 Other (please describe) \_\_\_\_\_**Personal Device Usage**

15. What percent of your employees handle Company business from their personal devices (select one)?

 We prohibit it I don't know Less than 25% 25 – 75% More than 75%

**Personally Identifiable Information (PII) Security**

16. a. Please estimate the annual volume of each type of information you process or store, taking into account both electronic and paper files as well as employee and customer information:
- SSN, individual taxpayer ID, driver's license, passport or federal ID numbers \_\_\_\_\_
- Payment card data (*credit or debit cards*) \_\_\_\_\_
- Protected health information \_\_\_\_\_
- Other confidential or protected information \_\_\_\_\_
- b. How long do you store the above records? \_\_\_\_\_ **Yes** **No**
- c. Do you have a record retention/destruction policy in place?
- d. Which controls are in place to protect PII in the Company's care, custody and control?
- Physical controls on access to computer systems and sensitive documents.
- Network segmentation of sensitive data
- Encryption policies
- Privilege management
- Annual employee security awareness training

**End Point Security**

17. Please indicate below the endpoint (*PC's, laptops, Smartphones, tablets, etc.*) security controls your Company is using:
- Password/passcode protected
- Encryption
- Firewalls enabled/turned on
- Traditional antivirus products on all endpoints
- Next generation antivirus on all endpoints
18. Who is primarily responsible for patching end points?
- A managed services provider  The Company's IT department  The user/employee

**Email Security**

- |  | <b>I Don't Know</b>      | <b>Yes</b>               | <b>No</b>                |
|--|--------------------------|--------------------------|--------------------------|
| 19. Do you use Sender Policy Framework (SPF)?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 20. How often is phishing training conducted to all staff:   |                          |                          |                          |
| <input type="checkbox"/> Never <input type="checkbox"/> I don't know <input type="checkbox"/> Semiannually <input type="checkbox"/> Annually |                          |                          |                          |
| 21. Do you use an email filtering tool to detect and/or block SPAM, malicious links, and attachments?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 22. Do you require multifactor authentication (MFA) to access email?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**Network Security**

- |   | <b>Yes</b>               | <b>No</b>                |
|---|--------------------------|--------------------------|
| 23. Is your network WiFi enabled?   | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>If yes</b> , please indicate level of WPA protocol: <input type="checkbox"/> WPA <input type="checkbox"/> WPA2 <input type="checkbox"/> WPA3 <input type="checkbox"/> I don't know |                          |                          |
| 24. Who monitors the Company's networks for intrusions or other unusual activity ( <i>select one</i> )?   |                          |                          |
| <input type="checkbox"/> Nobody/we do not monitor   |                          |                          |
| <input type="checkbox"/> Somebody in the Company's IT department  |                          |                          |
| <input type="checkbox"/> A third party/managed security provider  |                          |                          |
| <input type="checkbox"/> Somebody in the Company's IT department AND a third party/managed security provider  |                          |                          |

**Network Security Continued**

I Don't Know Yes No

- |  |   |   |                                |
|--|---|---|--------------------------------|
| 25. Are your firewalls configured according to the principles of least privileges?   |   | <input type="checkbox"/>                | <input type="checkbox"/>       |
| 26. Do you regularly review firewall rules and alerts?   | <input type="checkbox"/>                | <input type="checkbox"/>                | <input type="checkbox"/>       |
| 27. Is multi-factor authentication required to remotely connect to the network?  | <input type="checkbox"/>                | <input type="checkbox"/>                | <input type="checkbox"/>       |
| 28. When did the Company last have a comprehensive ( <i>i.e. inclusive of vulnerability scanning and penetration testing</i> ) network security assessment conducted by a third party ( <i>select one</i> )? |   |   |                                |
| <input type="checkbox"/> Last 6 months   | <input type="checkbox"/> Last 18 months | <input type="checkbox"/> Last 36 months | <input type="checkbox"/> Never |
| 29. Does the Company maintain a formal program for evaluating the security posture of its vendors?   |   | <input type="checkbox"/>                | <input type="checkbox"/>       |

**Back-Up Security**

Yes No

- |   |  |   |
|---|--|---|
| 30. Do you back up all mission critical systems and data?         | <input type="checkbox"/>                             | <input type="checkbox"/>                |
| <b>If yes</b> , please provide the following:                     |  |   |
| How Frequently do you back up?                                    | <input type="checkbox"/> Daily/nightly               | <input type="checkbox"/> Weekly         |
|   | <input type="checkbox"/> Less frequently then weekly |   |
| Which of the following back-up solutions do you employ?           |  |   |
|   | <input type="checkbox"/> Local                       | <input type="checkbox"/> Network drives |
|   | <input type="checkbox"/> Tapes/disks                 | <input type="checkbox"/> Off-site       |
|   | <input type="checkbox"/> Cloud                       |   |
| Which of the above are encrypted?                                 |  |   |
|   | <input type="checkbox"/> Local                       | <input type="checkbox"/> Network drives |
|   | <input type="checkbox"/> Tapes/disks                 | <input type="checkbox"/> Off-site       |
|   | <input type="checkbox"/> Cloud                       |   |
| How quickly can you restore from back-ups?                        | <input type="checkbox"/> Same day                    | <input type="checkbox"/> 24-48 hours    |
|   | <input type="checkbox"/> Longer                      |   |
| How frequently do you test your ability to restore from back ups? |  |   |
|   | <input type="checkbox"/> Never                       | <input type="checkbox"/> Quarterly      |
|   | <input type="checkbox"/> Semi-annually               | <input type="checkbox"/> Annually       |

**Web Hosting**

Yes No

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 31. Do you outsource your web hosting? | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

**Compliance**

- |   |  |                          |                          |
|---|--|--------------------------|--------------------------|
| 32. Are you compliant with the Payment Card Industry Data Security Standard (PCI-DSS) ( <i>select one</i> )?                        |  |                          |                          |
| <input type="checkbox"/> Yes  | <input type="checkbox"/> No  |                          |                          |
| <input type="checkbox"/> I don't know   | <input type="checkbox"/> We do not process ANY payment card transactions |                          |                          |
| 33. Does the Company maintain documented compliance programs for applicable laws/ rules/regulations such as HIPAA, GLBA, GDPR, etc? | I Don't Know   | Yes                      | No                       |
|   | <input type="checkbox"/>   | <input type="checkbox"/> | <input type="checkbox"/> |

**Media Content**

- |  |
|--|
| 34. The Company's attempts to mitigate its exposure to media liability by using the following controls ( <i>select all that apply</i> ): |
| <input type="checkbox"/> Obtaining all necessary rights to use third party content   |
| <input type="checkbox"/> Social media policy   |
| <input type="checkbox"/> Take-down procedures  |
| <input type="checkbox"/> Legal review of all materials   |

**Fraud Warning**

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

**Representations and Signatures**

The undersigned declares that to the best of his or her knowledge the statements set forth herein are true and correct and that reasonable efforts have been made to obtain sufficient information from each and every person and entity proposed for this insurance to facilitate the proper and accurate completion of this application. The undersigned further agrees that if any significant adverse change in the condition of the applicant is discovered between the date of this application and the effective date of the Policy, which would render this application inaccurate or incomplete, notice of such change will be reported in writing to the Insurer immediately. The signing of this application does not bind the undersigned to purchase the insurance.

It is agreed by the Company and the Insured Persons that the particulars and statements contained in this application and any information provided herewith (*which shall be on file with the Insurer and be deemed attached hereto as if physically attached hereto*) are the basis of this Policy and are to be considered as incorporated in and constituting a part of this Policy. It is further agreed that the statements in this application or any information provided herewith are their representations, they are material, and any Policy issued is in reliance upon the truth of such representations.

**Applicant Signature** \_\_\_\_\_ **Title** \_\_\_\_\_ **Date** \_\_\_\_\_

**Printed Name** \_\_\_\_\_

**Agent Name** \_\_\_\_\_ **Agent Signature** \_\_\_\_\_

**NOTE: This Application, including any material submitted herewith will be treated in strictest confidence.**

**Great American Insurance Group Cyber Risk Division****Canadian Branch of Great American Insurance Company**

Scotia Plaza, Suite 2100  
40 King Street West  
Toronto, Ontario M5H 3C2