CYBER LIABILITY APPLICATION

PLEASE ANSWER ALL QUESTIONS
IF THEY DO NOT APPLY, INDICATE "N/A" - IF SPACE IS INSUFFICIENT PLEASE USE SEPARATE SHEETS

Section A: General Information

1. a) **Name of Insured**: _____

b) **Mailing Address:**

c) Year established: _____

d) Current number of employees:
Canada: _____
U.S.: _____
Foreign: _____

e) Locations of overseas offices (please list countries):

2. a) Describe in detail your business activities:

b) Have you acquired or merged with any companies in the past 3 years? ☐ Yes ☐ No
If YES, please give details:

c) Do you anticipate any major changes in these activities in the next 12 months? ☐ Yes ☐ No
If YES, provide full details:

3. a) Please detail your revenue, including fees, for the past year, and estimated revenue for the current and next year:

Date of your financial year end: _____ Currency: _____

	Past year	**Current year (estimate)**	**Next year (estimate)**
Canada			
USA			
Rest of World (please list countries)			
Total			
Profit or (Loss)			

b) Please provide an approximate breakdown of your revenues by client type?

Corporate / B2B: _____ % Consumer / B2C: _____ %

4. Is the company part of any professional body or association? ☐ Yes ☐ No
If YES, please detail below:

5. Does the company possess any professional accreditation? ☐ Yes ☐ No
If YES, please detail below:

Section B: People

1. Can you confirm you adhere to the following best practices?

a) Have a dedicated individual responsible for Information Security and Privacy ☐ Yes ☐ No

b) Perform background checks on all employees and contractors with access to sensitive data ☐ Yes ☐ No

c) Perform background checks on all employees and contractors whose work involves critical IT infrastructure ☐ Yes ☐ No

d) Have restricted access to sensitive data (including physical records) to only those requiring it ☐ Yes ☐ No

e) Have a process to delete systems access within 48 hours after employee termination ☐ Yes ☐ No

f) Have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training ☐ Yes ☐ No

If NO to any of the above, please detail below along with mitigating comments:

2. Have you terminated the contract of any IT staff members in the last 12 months? ☐ Yes ☐ No
If YES, How many and which titles did they hold:

If YES, were any of these decisions made as a result of malicious or dishonest actions? ☐ Yes ☐ No
If YES, please provide more information:

Section C: Website

1. Please list your Website addresses and estimated current monthly unique visitors:

Website address	Estimated current monthly unique visitors

2. Please detail your website functionality: Tick if applicable

a) Basic brochure website ☐
b) Third party advertising on your website ☐
c) User content allowed (Chat rooms, bulletin boards, discussion forums, etc.) ☐
d) Large content volumes published ☐
e) Large media download / streaming volumes ☐
f) Client log-in area ☐
g) Transactional, accepting payment cards ☐

3. Do you publish third party content on your website? ☐ Yes ☐ No

If YES, do you have procedures in place, in respect of securing rights for using such content? ☐ Yes ☐ No

4. Does your website allow third parties to post comments or content directly to your website? ☐ Yes ☐ No

If YES, do you offer a mechanism for website viewers to flag content they are unhappy with? ☐ Yes ☐ No

Describe how you manage such issues when brought to your attention:

5. What percentage of your revenue emanates from online or e-commerce activities? _____ %

6. Typically, how often is your website changed in terms of content or functionality? Tick if applicable

a) Regularly (at least every few days) ☐
b) Weekly or Monthly ☐
c) Sporadically / When needed (not typically more than once per month) ☐
d) Are changes checked by a second person before "put live"? Yes ☐ No ☐

Section D: Network

1. If your IT network failed, which of the following would best describe the impact to your business?

   a) Inconvenience, very minimal revenue impact and operations could continue temporarily ☐
   b) Revenues would NOT be impacted immediately, and only slightly when impacted ☐
   c) Revenues would NOT be impacted immediately, but significantly when impacted ☐
   d) Revenues would be impacted immediately but only slightly ☐
   e) Revenues would be impacted immediately and significantly ☐
   f) Operations and revenues would be entirely interrupted ☐

   Please describe further:

2. Can you confirm you comply with the following minimum security standards?

   a) You use anti-virus, anti-spyware and anti-malware software ☐ Yes ☐ No
   b) You use firewalls and other security appliances between the Internet and sensitive data ☐ Yes ☐ No
   c) You use intrusion detection or intrusion prevention systems (IDS/IPS) and these are monitored ☐ Yes ☐ No
   d) You perform regular backups and periodically monitor the quality of the backups ☐ Yes ☐ No

   If NO to any of the above, please detail below along with mitigating comments:

3. In which timescales do you update anti-virus / anti-malware protections with patches? Tick if applicable

   a) As soon as practicable but always promptly, directly following patch release ☐
   b) Weekly or Monthly ☐
   c) Once per week ☐

   Less often than weekly (please detail timescale) ☐

4. Please provide details of the vendors for the following services (or check box if it is managed and operated in-house):

Client	Vendor	In-House
Internet Service Provider		☐
Cloud / Hosting / Data Centre Provider		☐
Payment Processing		☐
Data or Information Processing		☐
Offsite Archiving, Backup and Storage		☐
Other (please specify)		☐

5. Do you typically require such outsources providers to:

a) Demonstrate adequacy of IT Security and risk management procedures ☐ Yes ☐ No

b) Procure and evidence relevant insurance for the services they provide to you ☐ Yes ☐ No

c) Indemnify you contractually in respect of their errors or negligence (including data breach and system downtime) ☐ Yes ☐ No

If NO to any of the above, why not?

6. a) Do you have a written "data breach" or "privacy breach" response plan? ☐ Yes ☐ No

b) Have you tested this plan before? ☐ Yes ☐ No

c) Last date of test or regularity of testing? _____

7. Do you only use operating systems that continue to be supported by the original provider? If NO, please detail below along with mitigating comments: ☐ Yes ☐ No

8. Do you allow remote access to your Network?

☐ No

☐ Yes, to employees only

☐ Yes, to employees and other third parties

If YES, what security measures are utilized to keep such remote access secure?

9. a) What is the size of your dedicated IT budget annually? _____

   b) Approximate proportion dedicated to IT Security? _____

   c) Has this gone up or down in the past 3 years? _____

10. Are any major network / system IT changes envisaged or planned in the next 12 months? ☐ Yes ☐ No
    If YES, please detail fully:

11. Are annual or more frequent internal/external audit reviews (including penetration testing) performed on your IT network and your procedures? ☐ Yes ☐ No
    If YES, please provide a copy of the latest report from any examination/audit.

12. a) Do you have a Disaster Recovery Plan (DRP) and/or Business Continuity Plan (BCP) in place? ☐ Yes ☐ No

    b) In your DRP / BCP, how long would it take for you to be fully operational again following an incident? _____

    c) How often do you test your DRP / BCP? _____

    d) When did you last test your DRP / BCP? _____

13. Please describe your network contingency / redundancy / resilience in place to mitigate system interruptions or failures (such as mirrored infrastructure, failover mechanisms, warm or hot replicated sites or similar)?

Section E: Data

1. Do you hold or process any of the following types of sensitive CONSUMER data? Approx # of records

   a) Financial information (including credit/debit card records) ☐ Yes ☐ No _____

   b) Medical information ☐ Yes ☐ No _____

   c) Identity information (including NI number or passport details ☐ Yes ☐ No _____

   d) Names, addresses, telephone numbers ☐ Yes ☐ No _____

   e) What percentage of these individuals reside in the United States? _____ %

2. Do you hold or process any of the following types of sensitive corporate data? Approx # of records

   a) Confidential intellectual property / trade secrets ☐ Yes ☐ No _____

   b) Financial information ☐ Yes ☐ No _____

3. Do you utilize encryption in the following scenarios?

   a) Sensitive data is encrypted at rest within your network? ☐ Yes ☐ No

   b) Sensitive data is encrypted on backup tapes? ☐ Yes ☐ No

   c) Sensitive data is encrypted when transmitted outside of your network? ☐ Yes ☐ No

   d) Sensitive data is encrypted when transferred to portable media devices (USBs, Laptops, etc.)? ☐ Yes ☐ No

   If NO to any of the above, please provide mitigating comments:

4. Do you segregate data to mitigate the risk of large scale data loss from a single intrusion? ☐ Yes ☐ No
   If YES, please provide full details:

5. Do you monitor, restrict or block employees' ability to remove data via network end-points such as USB drives? ☐ Yes ☐ No

6. Do you have controls in place to restrict or control employees' ability to take physical data such as paper files away from your premises? ☐ Yes ☐ No

7. Please detail any salting or hashing techniques, or any other type of password cryptography you use:

Section F: Claims and Insurance History

1. Have you previously been insured for Cyber risks? ☐ Yes ☐ No
If YES, please provide the following unless you are currently insured with Markel:

Limit of Liability:		Insurer:	
Deductible:		Retroactive Date:	
Premium:		Expiry Date:	

2. Has any company declined to write, cancelled or non-renewed Cyber Liability cover for this company? ☐ Yes ☐ No
If YES, provide details:

3. Regarding all the types of insurance covers to which this Application relates, are you or any of the Partners, Principals, or Directors, after having made full enquiries, including of all staff, aware of any of the following matters?

a) Any claims (successful or otherwise) or cease and desist orders been made against the company, its predecessor, or present or past Partners, Principals, or Directors ☐ Yes ☐ No

b) Any circumstances which may give rise to a claim against the company, its predecessor, or any past or present Partner, Director, Principal or employee ☐ Yes ☐ No

c) Any loss or damage that has occurred to the company or its predecessor ☐ Yes ☐ No

d) Any privacy breach, virus, DDOS, or hacking incident which has, or could, adversely impact(ed) your business ☐ Yes ☐ No

e) Any evidence of network intrusion or vulnerabilities highlighted in an IT Security audit or Penetration test which have not yet been resolved ☐ Yes ☐ No

f) Any unforeseen down time to your website or IT network of more than 3 hours ☐ Yes ☐ No

If YES to any of the above, please provide full details:

THE UNDERSIGNED HEREBY ACKNOWLEDGES THE TRUTH OF THE STATEMENTS CONTAINED HEREIN.

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.

THE COMPLETION AND SIGNING OF THIS APPLICATION DOES NOT CONSTITUTE A PROMISE TO PROVIDE COVERAGE OR A BINDER OF INSURANCE. HOWEVER, IF A POLICY IS ISSUED, THIS APPLICATION SHALL SERVE AS THE BASIS OF SUCH CONTRACT AND WILL BE ATTACHED TO, AND FORM PART OF THE POLICY.

I AUTHORIZE YOU TO COLLECT, USE AND DISCLOSE PERSONAL INFORMATION AS PERMITTED BY LAW, IN CONNECTION WITH YOUR COMMERCIAL INSURANCE POLICY OR A RENEWAL, EXTENSION OR VARIATION THEREOF, FOR THE PURPOSES NECESSARY TO ASSESS THE RISK, INVESTIGATE AND SETTLE CLAIMS, AND DETECT AND PREVENT FRAUD, SUCH AS CREDIT INFORMATION, AND CLAIMS HISTORY.

For purposes of the Insurance Companies Act (Canada), this document was issued in the course of Lloyd's Underwriters' insurance business in Canada.

Signature of Applicant (authorized representative) Date

SUBMITTED BY: _____

EMAIL: _____

For contact information visit:
www.markelinternational.ca