Cyber Application

Complete this application in full and attach all required materials. If coverage is bound, this application and the materials submitted with it will be attached to the Policy and will constitute a part thereof

Section 1: Background Information

Name of Applicant:	Website Address(es):	Street Address:
City:	Province:	Postal Code:

Please provide the following information for all subsidiaries for which coverage is desired (attach a schedule if necessary):

Name Location Nature of Business Percentage owned by Applicant

1. Please provide the date the Applicant was established: _____

   Applicant is: ☐ Individual ☐ Partnership ☐ Corporation ☐ Other (specify): _____

   Number of employees: _____

   ☐ Public ☐ Private

2. Has the name of the Applicant changed in the last 12 months? ☐ Yes ☐ No

   Has the Applicant been involved in a merger, acquisition or consolidation with another entity in the last 12 months? ☐ Yes ☐ No

   Is the Applicant wholly or partly owned, controlled or related to any other entity? ☐ Yes ☐ No

   Does the Applicant own or control and other entity? ☐ Yes ☐ No

   If the Applicant responded "yes" to any part of question 2, please provide details:

3. Please describe the business services of the Applicant:

4. Please provide the revenue information based on the most recent financial year:

Gross Revenue	Past 12 Months	Current 12 Months	Project for Next Year
Canada			
USA			
Other			

Please attach a copy of the Applicant's most recent audited financials or the Applicant's current annual report.

5. a) Does the Applicant currently purchase this coverage?

Year	Coverage Type	Carrier	Limit	Deductible	Retroactive Date	Premium

b) Has any Errors or Omissions, Privacy, Cyber or Professional Liability Insurance ever been declined, cancelled or non-renewed? ☐ Yes ☐ No

If Yes, please explain:

_____

_____

Section 2: Controls & Procedures

1. Is there a risk assessment program that has been approved by management? ☐ Yes ☐ No

   If Yes, does it include any of the following? (check all that apply)

   - ☐ Communicated to appropriate constituents?
   - ☐ An owner to maintain and review the programs?
   - ☐ Risk assessment conducted in the last 12 months
   - ☐ Risk governance
   - ☐ Range of assets (including but not limited to: people processes, data and technology)
   - ☐ Range of threats (including but not limited to: malicious, natural, accidental, business changes)
   - ☐ Ownership, action plan, response plan, management update

2. What is the total IT budget dedicated to network security? (either percentage of revenues): _____
3. Does the Applicant have a specific individual responsible for overall privacy and security? ☐ Yes ☐ No
   a) Who is responsible for information assets?: _____
   b) Who is responsible for information security?: _____
4. Does the Applicant have a written corporate privacy policy which is reviewed by a qualified lawyer, actively followed and regularly updated? ☐ Yes ☐ No

   If Yes, when was it last updated? _____
5. Are employees required to review the corporate privacy policy and acknowledge they have read and accepted the terms and conditions? ☐ Yes ☐ No
6. Does the privacy policy communicate the acceptable use of data as well as detail disciplinary actions for failure to follow? ☐ Yes ☐ No
7. Is there training in place for employees with respects to privacy matters? ☐ Yes ☐ No

   If Yes, how often is training conducted? ☐ Monthly ☐ Quarterly ☐ Yearly ☐ Other: _____
8. Does this training include timely topics such as Phishing and Social Engineering? ☐ Yes ☐ No
9. Does the Applicant conduct screening of potential employees (e.g. background, drug, criminal, credit, etc.)? ☐ Yes ☐ No

10. Does the Applicant conduct regular network security assessments performed by third parties? ☐ Yes ☐ No

    a) When was the last assessment completed? _____

    b) Who performed the last assessment?: _____

    c) Is there a policy and procedure in place to respond to and rectify critical issues identified by an assessment in a timely manner? ☐ Yes ☐ No

11. Does the Applicant classify and track where sensitive data is processed on their network? ☐ Yes ☐ No

12. Does the Applicant follow any security frameworks in the development of overall security posture? (NIST, ISO 27000, COBIT, etc.) ☐ Yes ☐ No

13. Is the Applicant required to be Compliant with any of the following:

    a) FISMA ☐ Yes ☐ No ☐ N/A
    b) PHIPA/HIPAA/HITECH ☐ Yes ☐ No ☐ N/A
    c) PCI-DSS ☐ Yes ☐ No ☐ N/A
    d) SOX ☐ Yes ☐ No ☐ N/A
    e) PIPEDA/GLBA ☐ Yes ☐ No ☐ N/A
    f) Red Flag Rules ☐ Yes ☐ No ☐ N/A
    g) MA 201 CMR 17 or similar ☐ Yes ☐ No ☐ N/A
    h) COPPA ☐ Yes ☐ No ☐ N/A
    I) Other: _____

14. Does the Applicant have procedures to ensure compliance with privacy regulatory bodies, federal, provincial, territorial and state privacy laws and industry standards, as applicable? ☐ Yes ☐ No

    If the applicant is not compliant with any of the required statues above, please explain.

    _____

Section 3: Access to Data

1. Please provide details of the volumes of personally identifiable and sensitive information which is handled, processed or stored by or on behalf of the Applicant:

Type of Information	Number of records stored or processed annually	Encryption capabilities (YES / NO)				
		At rest	In Transit	In mobile devices	Back-up tapes	Cloud Storage
Social insurance numbers (SIN, social security numbers, government ID or driver license information		☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Financial information (e.g. banking information)		☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Payment card data* Merchant level: _____		☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Personal health information		☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Intellectual Property		☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Other (please specify):		☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No

a) Does the Applicant accept credit cards as a form of payment? ☐ Yes ☐ No

***If payment card data passes through or resides on the Applicant's network, please complete the Point of Sale Supplemental Application**

b) How much sensitive information resides on the Applicant's largest database/network?

☐ Less than 250,000 records ☐ 250,001-500,000 records ☐ 500,001-1,000,000 records
☐ 1,000,001-5,000,000 records ☐ 5,000,001-10,000,000 records

If more than 10,000,000 records, please provide estimate: _____

c) If data resides on the Applicant's network and is not encrypted, please provide details of other compensating controls in place to protect this data (i.e. tokenization):

2. Does the Applicant utilize permission-based access to its sensitive data and applications? ☐ Yes ☐ No

a) Is there a process in place to grant and approve access to sensitive information and systems? ☐ Yes ☐ No

b) How often are user access rights reviewed? ☐ Monthly ☐ Quarterly ☐ Annually

c) Are user access rights removed immediately upon termination? ☐ Yes ☐ No

3. Is personally identifiable information and sensitive information stored in a secure demilitarized zone (DMZ) that is segregated from the rest of the network? ☐ Yes ☐ No

a) Are corporate and operational network's segregated? ☐ Yes ☐ No

4. Is access to sensitive data logged and monitored? ☐ Yes ☐ No

a) Are logs hardened for forensic evaluation? ☐ Yes ☐ No

b) Do logs capture unauthorized alteration / tampering of data, systems and log files? ☐ Yes ☐ No

c) How long are logs maintained?: _____

5. Is multi-factor authentication used for remote access by employees and third parties? ☐ Yes ☐ No

Section 4: Information Security

1. Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? ☐ Yes ☐ No

If Yes, does the policy contain:

a) Responsibilities for Security Management? ☐ Yes ☐ No

b) The application of anti-virus software, including regularly updating and patching security systems as needed? ☐ Yes ☐ No

c) The use and application of intrusion detection and/or prevention software? ☐ Yes ☐ No

d) The use and application of firewalls to restrict network traffic? ☐ Yes ☐ No

e) The use and application of data loss prevention (DLP) software? ☐ Yes ☐ No

f) A policy around File Integrity Monitoring (FIM) to validate the operating system and application software files? ☐ Yes ☐ No

g) A System Information and Event Management system (SIEM) to aggregate and analyze security system data in real time? ☐ Yes ☐ No

h) Regularly scheduled vulnerability assessments and a process to prioritize and implement any critical or high security vulnerabilities in a timely manner? ☐ Yes ☐ No

2. Are physical controls in place to prevent unauthorized access to the Applicant's premises and network? ☐ Yes ☐ No

3. Does the Applicant currently use any software or systems that are no longer supported by the developer or manufacturer? ☐ Yes ☐ No

   a) If yes, is there a plan in place to remove the software / hardware from the network or has the Applicant purchased additional support from the developer / manufacturer? ☐ Yes ☐ No

4. Does the Applicant have a password policy in place to require strong passwords and that passwords should be updated on a regular basis? ☐ Yes ☐ No

Section 5: Vendor Management, Cloud & Mobile

1. Describe which services (if any) are outsourced?

Data back-up ☐ Yes ☐ No ☐ N/A Provider: _____	Payment processing ☐ Yes ☐ No ☐ N/A Provider: _____
Data hosting ☐ Yes ☐ No ☐ N/A Provider: _____	Physical security ☐ Yes ☐ No ☐ N/A Provider: _____
IT infrastructure ☐ Yes ☐ No ☐ N/A Provider: _____	Software development ☐ Yes ☐ No ☐ N/A Provider: _____
IT security ☐ Yes ☐ No ☐ N/A Provider: _____	Customer marketing ☐ Yes ☐ No ☐ N/A Provider: _____

If "yes" to any of the above, please list the critical service providers in the space provided and confirm PCI compliance of outsourced payment processor and include a copy of the most recent PCI Report on Compliance.

2. Does the Applicant have contracts in place with all third parties that have access to any sensitive information? ☐ Yes ☐ No

   a) Do the contracts contain hold harmless / indemnity clauses that benefit the Applicant? ☐ Yes ☐ No

   b) Do contracts require third parties to carry errors and omissions insurance? ☐ Yes ☐ No

   c) Do contracts require third parties to carry cyber insurance? ☐ Yes ☐ No

3. Does the Applicant have a formalized process to assess the risk management of potential vendors or outsources? ☐ Yes ☐ No

   a) Does the Applicant perform a risk management / security audit on their vendors and outsourcers that have access to systems and data on a regular basis? ☐ Yes ☐ No

4. Does the Applicant utilize services of a third party cloud provider for infrastructure, software, applications or data storage? If yes: ☐ Yes ☐ No

   a) Which services? ☐ Infrastructure ☐ Software ☐ Application ☐ Data Storage ☐ Other: _____

   b) Is the cloud: ☐ Private ☐ Public ☐ hybrid

   c) Does the Applicant ensure that the security controls are followed with respects to regulatory statues and industry standards such as PCI, PIPEDA, HIPAA, etc.? ☐ Yes ☐ No

d) In the event of a breach, does the Application require the cloud provider to indemnify the costs to investigate and notify individuals? ☐ Yes ☐ No

If No, please explain: _____

_____

5. Does the application have a Mobile Device Management (MDM) policy in place? ☐ Yes ☐ No
If Yes, does it include policies around:

a) Acceptable use? ☐ Yes ☐ No
b) Minimum password standards? ☐ Yes ☐ No
c) Encryption verification? ☐ Yes ☐ No
d) Sandboxing? ☐ Yes ☐ No
e) Bring Your Own Device (BYOD)? ☐ Yes ☐ No
f) Specific actions that organization may take in the event of a lost/stolen or compromised mobile device (e.g., remote disable, remote wipe, confiscation, termination)? ☐ Yes ☐ No

Section 6: Disaster Recovery & Incident Response

1. Has the Application performed a Business Impact Analysis (BIA) to determine and evaluate the potential effects of an interruption to critical business operation as a result of a disaster, accident, malicious attack or emergency? ☐ Yes ☐ No

2. Does the Applicant have a Business Continuity Plan in place? ☐ Yes ☐ No
a) Is the plan tested on a regular basis? ☐ Yes ☐ No
b) Is there an independent review of the plan? ☐ Yes ☐ No
c) Who performs the review? _____
d) When was the plan last tested? _____

3. If the Applicant suffered a network disruption, how long would it take to become fully operational?

☐ 1-4 Hours ☐ 4-8 Hours ☐ 8-12 Hours ☐ 12-24 Hours ☐ 24-48 Hours

4. Does the Applicant have a Disaster Recovery Plan in place? ☐ Yes ☐ No
a) Is the plan tested on a regular basis? ☐ Yes ☐ No
b) Is there an independent review of the plan? ☐ Yes ☐ No
c) Who performs the review? _____
d) When was the plan last tested? _____

5. Does the Applicant have a written incident response plan regarding how compromised personally identifiable information is handled? ☐ Yes ☐ No

If Yes, does it include:

a) An incident / event response team with defined roles and availability? ☐ Yes ☐ No
b) Formalized reporting and escalation procedures? ☐ Yes ☐ No
c) Is the plan tested on a regular basis via tabletop exercises? ☐ Yes ☐ No
d) When was this plan last tested? _____

Section 7: Content & Marketing

1. Please describe the Content produced, developed and / or used by the Applicant:

   _____

   _____

2. Does the Applicant ensure the proper rights are obtained when using Content developed by a third party? ☐ Yes ☐ No
3. Does the Applicant have all Content that it uses reviewed by a qualified lawyer? ☐ Yes ☐ No
4. Is there a formal procedure to respond to allegations of intellectual property infringement, libel, slander or violations of privacy? ☐ Yes ☐ No
   a) Does this include procedures to be compliant with the Copyright Modernization Act in Canada ("Bill C-11") or the Digital Millennium Copyright Act (DMCA) in the USA? ☐ Yes ☐ No
5. Does the Applicant ensure that consent is obtained from individuals when collecting personally identifiable information? ☐ Yes ☐ No
6. Does the Applicant have a privacy policy with respect to handling of customers' personal information which is clearly displayed on its' website? ☐ Yes ☐ No
   a) Has it been reviewed by a qualified lawyer and regularly updated? ☐ Yes ☐ No
7. Does the Applicant ensure that procedures are followed to ensure compliance with the Canadian Anti-Spam Legislation (CASL), Telephone Consumer Protection Act (TCPA), any other anti-SPAM statutes and any other consumer protection act? ☐ Yes ☐ No

Section 8: Loss History

1. Do any principals, directors, officers, partners, professional employees or independent contractors of the Applicant or any of the entities identified in Question 2) in Section 1. above for which coverage is desired, have knowledge or information of any act, error, omission, breach of duty, privacy breach, cease and desist letter, alleged breach of intellectual property rights, or any other circumstance which might reasonably be expected to give rise to a claim or incident that would be covered under the proposed insurance? ☐ Yes ☐ No
2. Is the Applicant aware of any release, loss or disclosure of personally identifiable information or confidential business information in the care, custody or control of the Applicant during the last three years? ☐ Yes ☐ No
3. Is the Applicant aware of any known network interruption, intrusion or unauthorized access, network extortion attempts or demands, virus or malicious code attack, denial of service (DoS) attack, or the loss or damage to the Applicant's network or data during the last three years? ☐ Yes ☐ No
4. Has the Applicant, or any of its predecessors in business, subsidiaries or affiliates, or any of the principals, directors, officers, partners, professional employees or independent contractors ever been the subject of a regulatory action as a result of the handling of sensitive data, including a civil investigative demand, consent order or investigation by the Office of the Privacy Commissioner of Canada, the United States Attorney General or other regulatory or industry body? ☐ Yes ☐ No
5. During the past five years, have any incidents occurred, or claims been made or legal action brought against the Applicant or any of the entities identified in Question 2) in Section 1. above, for which coverage is desired, or any predecessors in business, subsidiaries, affiliates or any principal, director, officer or professional employee? ☐ Yes ☐ No

6. Has the Applicant reported the matters listed in this Section 8, under Questions 1-5 to its current or former insurance carrier? ☐ Yes ☐ No

Note: *If any such incidents or claims exist, or any such facts or circumstances exist which could give rise to a claim or incident that would otherwise be covered under the proposed insurance, then those claims or incidents and any other claims or incidents arising from such facts or circumstances are excluded from the proposed insurance.*

If the Applicant responded "yes" to any part of Section 8, 1-6, please provide full particulars for each claim, incident, notice or circumstance including any losses paid by your current or former insurance carrier.

The undersigned on behalf of the Applicant declares that the statements set forth are true. The undersigned on behalf of the Insured agrees that if the information supplied on this Application changes between the date of this Application and the effective date of the insurance, they shall, in order for the information to be accurate on the effective date of the insurance, immediately notify the Insurer of such changes, and the Insurer may withdraw or modify any outstanding quotations or authorizations or agreements to bind the insurance. Signing of this Application does not bind the Applicant/Insured or the Insurer to complete the insurance contract, but it is agreed that this Application shall be the basis of the contract should a policy be issued, and it will be attached to and become part of the Policy. All written statements and materials (including any information provided in the attached Appendices) furnished to the Insurer in conjunction with this Application are hereby incorporated by reference into this Application and made a part hereof. Any failure to provide accurate answers or any incorrect responses in the sections above may result in the nullification of any insurance policy issued by the Underwriters for this risk.

Applicant's Signature: _____

Must be signed by an Officer of the Applicant

_____

Print Name and Title Date (Mo./Day/Yr.)