Epack 3

New Business Application
Cyber Long Form

Instructions for Completing this Application

This is a fillable PDF Document.

Please answer all questions fully. If necessary, as noted in the questions below, please provide additional responses in a supplemental document on your letterhead attached to this Application.

Upon completion the Application must be signed and dated by an authorized representative of the Applicant.

NOTICES

Please note that the insurance coverage to which this Application applies provides that the policy limit available is reduced by amounts incurred for legal defence costs and expenses and may be completely exhausted by such amounts. CNA will not be liable for any defence costs or expenses, nor any settlement or judgment amount after the exhaustion of the policy limit. Please also note that amounts incurred for defence costs and expenses will be applied to the applicable retention. This Notice is subject to the provisions of the Quebec Civil Code where applicable to an issued policy.

Providing information about a claim, potential claim, first party loss, or potential first party loss in response to any question in any part of this Application does not create coverage for such claim, potential claim, first party loss, or potential first party loss. The Applicant's failure to report to its current insurance company any claim made against it or any first party loss it first discovered during the current policy period, or to report any act, omission, or circumstance of which the Applicant is aware that may give rise to a claim or first party loss, before expiration of the current policy, may create a lack of coverage.

Please note that the submission of a completed, signed Application does not result in an obligation to purchase insurance or an obligation by the insurance company to bind insurance.

I. APPLICANT INFORMATION

The Applicant to be named in Item 1. of Declarations (the "named insured"): _____

Address: _____

City: _____ Province: _____ Postal Code: _____

Website(s): _____ Telephone Number: _____

a. Date the Applicant was established: _____

b. Ownership Structure: ☐ Private ☐ Public ☐ Not-for-Profit ☐ Governmental

c. Business Type: ☐ Corporation ☐ Partnership ☐ Joint Venture ☐ LLC

d. Number of Employees: _____

e. Are you seeking coverage for any other "Named Insureds" and/or subsidiaries, affiliates, or other related entities? ◯ Yes ◯ No
If you answered "Yes" above, please attach details.

f. Is the Applicant wholly or partially owned or controlled by any other entity? ◯ Yes ◯ No
If you answered "Yes" above, please provide the name, date established, location, and degree of control for each such entity:
_____

g. Does the Applicant, either in whole or part, own, control, manage or operate any other entity not previously listed in this Application? ◯ Yes ◯ No
If you answered "Yes" above, please provide complete details: _____

h. Area or territory of operations: ☐ Local ☐ Regional ☐ National ☐ International

i. What is the nature of the Applicant's business? _____

II. COVERAGE REQUESTS

Coverage	Limit	Retention	Retroactive Date
Cyber	$ _____	$ _____	_____

III. EXPIRING COVERAGE INFORMATION

1. Please complete the following for those coverages for which you are currently insured:

Coverage	Limit	Retention	Retroactive Date	Premium	Carrier	Expiration Date
Cyber Liability	$ _____	$ _____	_____	$ _____	_____	_____

2. Has the insurer under any of the coverage listed above indicated an intent not to offer renewal terms? ◯ Yes ◯ No

IV. GENERAL INFORMATION

In the next 12 months (or during the past 18 months), indicate whether the Applicant or any Subsidiary has experienced, or anticipates any of the following:

a. Merger, consolidation, acquisition, or divesture? ◯ Yes ◯ No

b. Material changes in nature or size of operations? ◯ Yes ◯ No

c. Bankruptcy filing or re-organization? ◯ Yes ◯ No

If you answered "Yes" to any of the above, please provide complete details (if additional space is needed, please attach separately):

_____

V. FINANCIAL INFORMATION

1. Please indicate the Applicant's Gross Annual Revenue

Prior Year	Current Year	Projected
$ _____	$ _____	$ _____

2. Please indicate the percentage of the Applicant's revenue generated inside Canada versus the percentage generated outside of Canada:

Canada: _____% US: _____ % Foreign: _____ %

VI. CLAIMS INFORMATION

1. Has notice of any claim, potential claim, first party loss (including but not limited to data breach, security breach, extortion threat/demand, or release/loss/disclosure of or unauthorized access to personally identifiable information in the Applicant's care, custody, or control), or potential first party loss, been given to any insurer for any coverage for which the Applicant is applying? ◯ Yes ◯ No

2. Within the past 3 years, has the Applicant, any Subsidiary, or any person associated with such entities for whom this insurance is being sought ("Proposed Insureds"), been the subject of, or involved in, any claim, written demand, notice, proceeding, litigation, or investigation alleging:

   a. Violations of any privacy or data security laws or regulations? ◯ Yes ◯ No

   b. Privacy injury, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks, or the inability of the Applicant's or Subsidiary's authorized users to access the Applicant's or Subsidiary's network? ◯ Yes ◯ No

   c. A loss of money, securities, or property due to social engineering, fraud, or other criminal acts? ◯ Yes ◯ No

3. Within the past 3 years, has any Proposed Insured been the subject of any inquiries, investigations, or disciplinary action by a regulatory or administrative agency or association? ◯ Yes ◯ No

4. Within the past 3 years, has any Proposed Insured been made aware of any potential first party loss (including but not limited to data breach, security breach, extortion threat/demand, or release/loss/disclosure of or unauthorized access to personally identifiable information in the Applicant's care, custody, or control), whether or not reported to a prior insurer? ◯ Yes ◯ No

If you answered "Yes" to any of the questions in paragraphs 1. through 4. above, please provide details, including date, type of claim or first party loss, allegations, current status, defence costs incurred, and any judgment or settlement amounts. (If additional space is needed, please attach separately):

_____

VII. CYBER COVERAGE PART

A. Sensitive Information

1. Please identify any sensitive employee, customer, or client information that the Applicant has possession of:

Type of Information	Estimated Number of Records	Are These Records Encrypted at Rest	Are These Records Encrypted in Transit
Social Insurance Numbers	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Driver's Licence Numbers	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable

Financial Account Numbers	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Credit Card Numbers	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Personal Health Information	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Biometric Data	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Third Party Trade Secrets	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Third Party Intellectual Property	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Third Party Corporate Financial Information	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable
Total	_____	◯ Yes ◯ No	◯ Yes ◯ No ◯ Not applicable

2. Is there any segregation of the data discussed in question 1 above? ◯ Yes ◯ No
   If you answered "Yes" above, what is the largest number of records stored in one place?_____

3. Is any of the information discussed in question 1 above stored on mobile devices (i.e. laptops, tablets, mobile phones, etc.)? ◯ Yes ◯ No
   If you answered "Yes" above, is it encrypted at rest and in transit? ◯ Yes ◯ No

4. Is any of the above information discussed in question 1 above from non-Canadian residents or non-Canadian domiciled companies? ◯ Yes ◯ No ◯ N/A

B. Information Security and Privacy Policies

1. Please indicate if the Applicant:	Yes	No
a. Has a specific individual responsible for overall privacy and information security?	◯	◯
b. Has a specific individual responsible for monitoring changes in statutes and regulations related to privacy and information security?	◯	◯
c. Has formal written information security and privacy policies, standards, and/or procedures for the administration of information security throughout your organization?	◯	◯
d. Has a written records retention policy that includes the secure disposal/deletion of paper/ electronic records, biometric information, and data when no longer needed?	◯	◯
e. Stores data only as necessary for the performance of services?	◯	◯
f. Has had the information security and privacy policies been reviewed by an outside counsel specializing in privacy law?	◯	◯
g. Has a formal security awareness and education program to support and communicate new and existing standards and policies to employees?	◯	◯
h. Requires that every person in the organization be given anti-fraud security awareness training on an ongoing basis that includes but is not limited to detection of social engineering, phishing or other similar scams?	◯	◯
i. Has a formal and comprehensive employee on-boarding process (including background checks, drug tests, criminal, credit, etc.)?	◯	◯

2. Is the Applicant in compliance with:	Yes	No	NA
a. PIPEDA or any substantially similar provincial privacy or health privacy legislation or regulations	◯	◯	◯
b. EU General Data Protection Regulation?	◯	◯	◯
c. Health Insurance Portability and Accountability Act (US)?	◯	◯	◯
d. California Consumer Privacy Act	◯	◯	◯
e. Any federal, provincial or territorial or state biometric information statute or regulation?	◯	◯	◯

C. Network Security Controls

1. Does the Applicant:	Yes	No
a. Utilize any unsupported operating systems? (e.g. Windows XP, or Server 2003)	☐	☐
b. Assess applications and infrastructure for common security vulnerabilities (e.g. OWASP top 10, SANS 20)?	☐	☐
c. Replace factory default settings (including user names and passwords) to ensure your information security systems are securely configured?	☐	☐
d. Implement segregation of duties for development, testing, and production environments?	☐	☐
e. Check for security patches to your systems at least weekly and implement them within 30 days?	☐	☐
If you answered "No", please provide an overview of your patching process: _____		

2. How often does the Applicant have third parties conduct regular network and application penetration tests? _____

3. Have all medium/high/critical findings in the most recent test been remediated? ☐ Yes ☐ No

4. How often does the Applicant perform formal risk assessments? _____

5. Does the Applicant perform regular backups of data, applications, and system configurations? ☐ Yes ☐ No

   If you answered "Yes" above, are the backups:

   a. Regularly tested to ensure restorability? ☐ Yes ☐ No

   b. Stored offsite and offline? ☐ Yes ☐ No

   c. Encrypted at rest? ☐ Yes ☐ No

6. Does the Applicant have the following in place:	Yes	No
a. Up to date Anti-Virus Software?	☐	☐
b. Multi Factor Authentication for remote connection to the Applicant's network?	☐	☐
c. Multi Factor Authentication for privileged user access?	☐	☐
d. Virtual Private Network (VPN), SSL VPN or equivalent technology?	☐	☐
e. A Security Information and Event Management (SIEM) system?	☐	☐
f. Data Leakage Prevention technology or other similar programs/technologies?	☐	☐
g. Wi-Fi- Protected Access 2 Authentication and Encryption or stronger on the Applicant's wireless network?	☐	☐
h. Password practices and controls (i.e. minimum password length, characters and/or capitalized letters?	☐	☐

7. Does the Applicant:	Yes	No
a. Control access to your system to ensure that users only have access to the appropriate environments necessary for their work?	☐	☐
b. Audit user access to ensure no authorization has been granted that exceeds employees' job responsibilities?	☐	☐
If you answered "Yes", how often? _____		
c. Timely remove systems access when an individual leaves the organization and/or when access is no longer required for business purposes?	☐	☐
What is the time frame? _____		
d. Limit physical access at all locations to your own personnel and only authorized sub-contractors, agents, or visitors?	☐	☐

8. Does the Applicant enforce the following for access control to data centers and networking closets:	Yes	No
a. Badge access	☐	☐
b. Biometrics	☐	☐
c. Automatic locking	☐	☐
d. Time alarms for open doors	☐	☐

D. Incident Response/Business Continuity/Disaster Recovery Plans

1. Does the Applicant have any of the following formal plans in place:

   a. Incident Response Plan in place? ☐ Yes ☐ No

   b. Business Continuity Plan in place? ☐ Yes ☐ No

   c. Disaster Recovery Plan in place? ☐ Yes ☐ No

   If you answered "Yes" to any of the above, how often are these plans tested? _____

2. 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 ☐ 48+ hours

E. Third Party Vendors and Service Providers

1. Whenever the Applicant entrusts sensitive information to 3rd parties does the Applicant:	Yes	No
a. Contractually require all such third parties to protect this information with safeguards at least equivalent to the Applicant's safeguards?	☐	☐
b. Perform due diligence on each such third party to ensure that their safeguards for protecting sensitive information meet the Applicant's standards (e.g. conduct security/privacy audits or review findings of independent security/privacy auditors)?	☐	☐
c. Audit all such third parties at least once a year to ensure that they continuously satisfy the Applicant's standards for safeguarding sensitive information?	☐	☐
d. Contractually require in writing that they defend and indemnify the Applicant if they contribute to a confidentiality, security, and/or privacy breach?	☐	☐
e. Require all such third parties to either have sufficient liquid assets or maintain enough Errors & Omissions insurance to cover their liability arising from a breach of privacy or confidentiality?	☐	☐
f. Request SOC 2 reports?	☐	☐

2. Current Network and Technology Providers (If applicable)

Internet Service Provider (s) _____

Cloud Services Provider (s) _____

Website Hosting _____

Collocation Services _____

Credit Card Processor(s) _____

Managed Security Services _____

Other(s) _____

3. What percentage of the Applicant's revenue is directly dependent on public facing websites? _____%

4. What is the minimum length of system outage for which the Applicant would anticipate a measurable impact on revenue? _____

F. Personal Health Information

1. Does the Applicant process, transmit, store, or use Personal Health Information (PHI)? ◯ Yes ◯ No

2. If you answered "Yes" to the above	Yes	No
a. Is a risk analysis performed to determine where PHI is being used and stored to identify the gaps and possible threats to said PHI?	◯	◯
b. Is access to PHI data/information restricted to only those that need access?	◯	◯
c. Is there a PHI specific incident response plan in place?	◯	◯
d. Are users trained on PHI security?	◯	◯
e. Are the information security and privacy controls discussed above in place and applicable to PHI in the Applicant's possession or control?	◯	◯

G. Payment Card Information

1. Does the Applicant accept payment via credit/debit card? ◯ Yes ◯ No

   If you answered "No" above, please skip to Section H, Cyber Crime.

2. Has the Applicant confirmed the Applicant's compliance with the PCI DSS (Payment Card Industry Data Security Standard)? ◯ Yes ◯ No

   a. If so, which version of the PCI Standard is the Applicant compliant with? _____

   b. How many transactions does the Applicant conduct on an annual basis? _____

   c. On what percentage of the Applicant's transactions is Europay, MasterCard, Visa (EMV Chip and Pin) or such similar tokenization used? _____%

3. If you answered "Yes" to the above:	Yes	No
a. Is segmentation used to isolate PCI information from the rest of the corporate network?	◯	◯
b. Is Tokenization used to remove the actual credit card number from the transaction?	◯	◯
c. Is there a policy and procedure for deploying patches to the point of sale devices?	◯	◯
d. Are connectivity restrictions in place to disallow internet?	◯	◯
e. Are the point of sale devices hardened via application whitelisting?	◯	◯
f. Is end to end encryption utilized from the moment credit card information is read into the point of sale device?	◯	◯

4. Please indicate if the following information is in custody, care or control:	Yes	No
a. Credit card data for the duration of a transaction	◯	◯
b. Credit card data stored for future use (all but last 4 digits masked)	◯	◯
c. Credit card data stored for future use (un-masked card numbers including track 2 data)	◯	◯

H. Cyber Crime

(to be completed only if the Applicant is seeking Cyber Crime coverage)

1. Does the Applicant:	Yes	No
a. Have procedures in place to verify the receipt of inventory, supplies, goods or services against an invoice prior to paying a vendor?	◯	◯
b. Have a written policy regarding electronic fund transfers?	◯	◯

c. Accept funds transfer instructions or changes to account details from internal sources (employees, etc.) or external sources (customers, vendors, etc.) over the telephone, fax, email or some other electronic communications method? ☐ ☐

If you answered "Yes", prior to complying with the instruction, does the Applicant authenticate such instructions using a method other than the initial contact method? ☐ Yes ☐ No

d. Limit authority to execute electronic transfers to specified employees? ☐ ☐

e. Restrict access to the online banking portal used to conduct electronic transfer functions to specific users and terminals? ☐ ☐

f. Require dual authorizations for payments or funds transfers of a certain amount? ☐ ☐

If you answered "Yes", what is that amount? $ _____

g. Have different policies and procedures for international electronic fund transfers? ☐ ☐

If yes, please explain in an attachment to this application?

2. What is the average monthly number of fund transfers? _____

3. What is the average dollar amount of an individual fund transfer? $ _____

4. What is the largest single amount that can be transferred? $ _____

APPLICANT REPRESENTATION

(To Be Completed by Applicant)

The Applicant Representation applies to all coverages that have been completed as part of this Application.

1. Special Representation applicable to the following Coverages only (if to be part of this policy):

For the coverage checked below, the Applicant has current coverage in place with either CNA or with any other carrier:

Coverages	Coverage has been in place since:
☐ Cyber	_____

The Applicant requests continuity for this coverage and this Applicant Representation does not apply to this coverage.

If no checkbox is checked above then this Applicant Representation applies to the coverage for which the Application has been completed subject to the following:

Applicant Representation - None of the individuals to be insured under the Cyber Coverage Part is responsible for or has knowledge of any wrongful act or fact, circumstance, or situation which they have reason to believe might result in a future claim or first party loss, except as follows:

☐ Yes, there are exceptions to this Representation (please attach details)

☐ No, there are no exceptions to this Representation

If any wrongful act or fact, circumstance, or situation which the Applicant has reason to believe might result in a future claim or first party loss whether not disclosed above, then the Applicant acknowledges and agrees, unless the proposed insurance policy expressly provides otherwise, any loss, claim, action, or first party loss arising out of, based upon, or attributable to such wrongful act or fact, circumstance, or situation will be excluded from coverage in accordance with the Application provision of the proposed policy.

2. Representations applicable to all coverages to be made part of this policy:

The Applicant hereby declares, after diligent inquiry, that the information contained herein and in any supplemental applications or forms required hereby are true, accurate, and complete, and that no material facts have been suppressed or misstated. The Applicant acknowledges a continuing obligation to report to the CNA Company (the "Company") to whom this Application is made, as soon as practicable, any material changes in all such information after signing the Application and prior to issuance of the

policy. The Applicant further acknowledges that the Company will have the right to withdraw or modify any outstanding quotations and/or authorizations or agreement to bind the insurance based upon such changes.

Further, the Applicant understands and acknowledges that:

a. Completion of this Application and any supplemental applications or forms does not bind the Company to issue a policy;

b. If a policy is issued, the Company has relied upon, as representations, this Application, any supplemental application, and other statements furnished to the Company in conjunction with this Application;

c. All supplemental applications, statements, and other materials furnished to the Company in conjunction with this Application are hereby incorporated by reference into this Application and made a part hereof;

d. This Application will be the basis of the contract and will be incorporated by references into and made a part of such policy;

e. If a policy is issued, the limit of liability contained in the policy will be reduced and may be completely exhausted by the payment of loss, defense costs, and expenses. In such event the Company will not be liable for loss, defense costs, and expenses to the extent that such loss, expenses, and defense costs exceed the limit of liability of this policy;

f. If a policy is issued, defence costs and expenses incurred will be applied against the deductible or retention amount as provided in the policy;

g. The Applicant's failure to report to its current insurance company:

   i. any claim made against it or any first party loss it discovered during the current policy term; or

   ii. any act, omission, or circumstances which the Applicant is aware of that may give rise to a claim or first party loss; before expiration of the current policy may create a lack of coverage.

FRAUD NOTICE

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

The Applicant, through the undersigned authorized representative, hereby acknowledges that the aforementioned statements and answers are accurate and complete. Applicant further understands that any inaccurate or incomplete statements may result in an exclusion or denial of insurance coverage. Applicant further authorizes CNA Insurance Companies to release the information on this Application and associated underwriting information.

Applicant:

By: _____ _____

*Signature and Title** *Printed Name of Authorized Representative*

Date: _____

*** This Application must be signed by the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, General Counsel or Risk Manager of the Applicant acting as the authorized representatives of the person(s) and entity(ies) proposed for this insurance. Please print and sign this application.**

Note: For purposes of the Insurance Companies Act (Canada), this document was made in the course of Continental Casualty Company's insurance business in Canada.