



Cyber, data and privacy

Notice: The policy for which these questions are made is a claims-made and reported policy subject to its terms. The questions contained herewith pertain to all persons or entities seeking insurance, and not just the signatory.

Details:

Brokerage Name:			
Producer Name:		Producer Email:	

Customer Details:

Company Name:			
Contact Name:		Contact Email:	
Address:			
Website:			
Gross Annual Revenue:	CAD \$	What percentage of Revenue is generated from the USA?	%
Industry/Business Sector:			
Does the applicant's business operate as any of the following restricted industries?	Adult pornography; Airline and airport operations; Blockchain technology provider; Business process outsourcing services; Call center services; Credit intermediation, Commodities and securities exchanges; Cryptocurrency activities; Data warehouse; Family planning or substance abuse centre or service, Adoption agency or abortion clinic; Franchisees/Franchisor; Gambling Industries; Government agency, Municipality or public body; Healthcare exchange or clearing house; Hotel or bed and breakfast; H.R. services, Insurance carrier; Managed IT Services; Marijuana and cannabis related products and services; Mobile Application or Video Game Development; Mortgage & loan broker; Payment Card Processor or Gateway; Payroll Processing; Securities intermediation; Social Dating or Professional Networking Services; Utilities including water or sewage provider; Broadcasters; Film Production/Publishers; <input type="checkbox"/> Yes <input type="checkbox"/> No		
Number of Records: For how many people (including customers, employees, and suppliers) do you process, transact, or store Personal Identifiable Information?			
Please select from the drop-down list:			

Create your preferred Cyberboxx Option:

Select Coverage Limit:	\$250,000, \$500,000, \$1,000,000 or \$2,000,000	
Add Cyber Crime & Fraud	\$100,000 or \$250,000	
Select Retention:	\$2,500, \$5,000, \$10,000 or \$25,000	

Security Controls:

Please read these questions and statements carefully. You must provide us with accurate and complete information. Failure to do so may affect the validity of the policy or whether the policy responds to any claim in full or at all.

The applicant has implemented commercially available firewalls and antivirus software on all computers, and updates these at least every 30 days.	<input type="checkbox"/> Yes <input type="checkbox"/> No
The applicant regularly back-ups critical data for on-premises systems at least weekly AND stores off-site OR critical data is stored exclusively with cloud software providers.	<input type="checkbox"/> Yes <input type="checkbox"/> No

The applicant limits access to all sensitive information to only those that need it to perform their function, and has a policy in place to ensure access is immediately amended or revoked for joiners, movers, and leavers	<input type="checkbox"/> Yes <input type="checkbox"/> No
The applicant has a process in place to regularly patch all systems and applications at least every 30 days.	<input type="checkbox"/> Yes <input type="checkbox"/> No
The applicant changes all default passwords on new devices and has a formal password policy that explains good password hygiene for all systems providing access to personal or confidential information.	<input type="checkbox"/> Yes <input type="checkbox"/> No
The applicant confirms that multi-factor authentication is always enabled on emails and remote access. (If 'No' see below)	<input type="checkbox"/> Yes <input type="checkbox"/> No

Notice: The policy for which these questions are made is a claims-made and reported policy subject to its terms. The questions contained herewith pertain to all persons or entities seeking insurance, and not just the signatory.

The applicant confirms that multi-factor authentication will be enabled on emails and for remote access within 30 days of binding this policy.	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

For Financial Crime and Fraud coverage :	<input type="checkbox"/> Yes <input type="checkbox"/> No
All employees responsible for wire transfer of funds are provided training to detect and prevent fraud, social engineering, and similar scams?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has specific financial crime training been provided to anyone who has authority to make payments greater than \$2,000?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do you require two parties to sign off on any payment transfers greater than \$2,000?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do you have policy in place to verify any changes to existing invoices, bank deposit information and contact information?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Before processing a payment or changing vendor account details do you make an answered telephone call to the number held on file for the third party/authorised person in order to verify the instructions are legitimate?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Prior Claims: During the past 5 years, has the applicant:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suffered any loss or had any claim, whether successful or not, made against them?	
Been investigated in respect to personal data, including but not limited to payment card information, or privacy practices?	
Been asked to supply any regulator or similar body with information relating to personally identifiable information or privacy practices?	
Received any complain relating to the handling of someone's personally identifiable information?	
Received any actual or attempted extortion demand with respect to its data or computer system?	

Is the applicant aware of anything that may lead to a claim, loss, or other liability that might be covered under this policy?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Important:

<p>You further confirm and agree that:</p> <p>You, and your insurance broker on your behalf, have given a fair presentation of the risk to be insured by disclosing all material facts and circumstances.</p> <p>You have provided consent for BOXX Insurance Inc. to use your information i) for underwriting purposes, including a cyber security rating through an external, non-intrusive source, ii) to compile aggregate statistical data to be used to monitor trends in the insurance industry, and iii) to comply with regulatory oversight.</p> <p>You comply with sanctions imposed by Canada, the United Kingdom, the European Union, and the Office of Foreign Asset Control. You understand that these sanctions prevent us from contracting with companies who are restricted under these Acts.</p> <p>Any matters pertaining to the Claims and knowledge disclosure above, shall be excluded from the proposed insurance (whether disclosed or otherwise).</p> <p>By entering your name and email, you agree that all information provided to BOXX Insurance to generate this insurance policy is accurate and true. Entering your name and email address is akin to signing any legal document and you will be bound to all acknowledgements provided herein and that you have the authority to bind your company to this agreement.</p> <p>Any quotation offered based on the above information, expires within thirty (30) days or on the expiration date of the current coverage, whichever comes first.</p>		
Your Name & Title:		
Signature:		
Email:		Dated:

For more detailed information on how we use your information, please review our [Privacy Policy](http://www.cyberboxx.ca/privacypolicy) (www.cyberboxx.ca/privacypolicy)