

	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?	
		What percentage of Revenue is generated from online sales?	
Industry/Business Sector:			
Business Description:			
Does the applicant conduct business within 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; 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.		
	<input type="checkbox"/> Yes <input type="checkbox"/> No		

Create your preferred Cyberboxx option:

Select Coverage Limit:	\$250,000, \$500,000, \$1,000,000, \$2,000,000 or \$5,000,000	Please select from the drop-down list:	
Add Cyber Crime & Fraud Sub Limit	\$100,000 or \$250,000	Please select from the drop-down list:	
Select Deductible	\$10,000, \$25,000, \$50,000, \$100,000	Please select from the drop-down list:	

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.

1.0 Data Privacy		
1.1	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:	
1.2	Please provide details of personal information (in both electronic and non-electronic form) you process or store using the following table. N.B. this should include information relating to employees (past, present and prospective), as well as third parties. <ul style="list-style-type: none"> a) Names, addresses and email addresses b) Individual taxpayer ID/ social security numbers / driving licenses / passport information c) Financial account records / payment card data 	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <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.

1.3	Have you conducted a review to determine what personal data you handle and where it is stored?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.4	Has a third-party audited your privacy practices and/or network security in the last two years? If yes, have you complied with all the recommendations provided?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
1.5	Do you obtain explicit consent from customers when collecting personal data?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.6	Do you maintain a written policy that addresses information security which is communicated to all employees?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.7	Do you mandate information security training for staff that have access to your information resources on at least an annual basis?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.8	If you use third parties to host your data, do they comply with any information security frameworks or information management schemes?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.9	Do you have a written privacy policy that has been reviewed by a suitably qualified lawyer?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.10	Do you accept credit card payments in your facilities or via the web? If yes, please answer the following questions:	<input type="checkbox"/> Yes <input type="checkbox"/> No
	<ul style="list-style-type: none"> • Do you outsource all your payment processing to a PCI-DSS compliant third party? • Do you ever store or transmit credit card details on your network, even momentarily? 	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No

2.0 Security Controls & Network Governance

2.1	Is there an individual in your organisation specifically assigned responsibility for information security such as a CISO?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.2	Do you have an incident response plan or other processes for responding to a cyber security incident? Has been tested in the last 12 months?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
2.3	Have you installed and do you maintain firewall configuration to protect your data and network?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.4	How frequently are software patches applied (including mission-critical or revenue-generating systems)? Please select from the drop-down list:	
2.5	Have you installed physical controls to protect sensitive systems and sensitive physical information under your care, custody, or control?	<input type="checkbox"/> Yes <input type="checkbox"/> No Add Details on supp page
2.6	Do you have procedures in place to restrict or remove login credentials of employees immediately following an employee's departure from your organisation?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If you have answered no to any of the above, please provide additional information.		

3.0 Ransomware Protection

3.1	Do you pre-screen emails for potentially malicious attachments and links?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.2	Do you restrict access to all sensitive information stored by you on a need to-to-know basis?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.3	The applicant confirms that multi-factor authentication is always enabled on emails and remote access. Please select from the drop-down list:	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.4	Do you have established processes for rapidly applying critical security patches across servers, laptops, desktops, and managed mobile devices?	<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.

3.5	Does your employee cyber security awareness program include phishing training and testing?	Annual Training <input type="checkbox"/> Yes <input type="checkbox"/> No Phishing Testing <input type="checkbox"/> Yes <input type="checkbox"/> No
3.6	Are all computer devices protected by anti-virus or endpoint protection software?	<input type="checkbox"/> Yes (Endpoint) <input type="checkbox"/> Yes (AV) <input type="checkbox"/> No
3.7	Do you have any internet facing open RDP ports?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If you have answered no to any of the above, please provide additional information.		

4.0 Business Interruption		
4.1	Do you maintain redundant back-ups of sensitive and critical system information?	<input type="checkbox"/> Yes (Offsite) <input type="checkbox"/> Yes (Onsite) <input type="checkbox"/> No
4.2	Are restore procedures documented and tested?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.3	Do you use credentials unique to backups that are stored separately from other user credentials?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.4	If you rely on third party hosting to conduct sensitive or critical information, do you have an alternative solution in the event of a provider failure?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4.5	Do you have protocols for replacement of end-of-life system/network equipment?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.6	Are your critical information/SCADA equipment, segregated from the wider IT environment with internal firewalls and software protection?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.7	Are any of these critical systems connected to the Internet?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.8	Do you segregate your network by geography, to isolate any potential malware infections?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.9	If so, how quickly can you obtain back-ups stored by third parties?	<input type="checkbox"/> 24 hours <input type="checkbox"/> One week <input type="checkbox"/> One month <input type="checkbox"/> Unknown
4.10	Do you have a disaster recovery plan and/or incident response plan that takes account of loss of functionality/data as a result of a hack, including provision to notify those affected if their personal data is compromised?	Neither <input type="checkbox"/> DRP <input type="checkbox"/> IRP <input type="checkbox"/>
If you have answered no to any of the above, please provide additional information.		

5.0 Cyber Crime and Fraud (if selected)		
5.1	Are 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
5.2	Before processing a wire transfer of funds OR changing vendor account details, do you confirm the request by a secondary means of communication?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If you have answered no to any of the above, please provide additional information.		

6.0 Prior Claims		
6.1	<p>Prior Claims: During the past 5 years, have you:</p> <ul style="list-style-type: none"> a) Suffered any loss or had any claim, whether successful or not, made against them? b) Been investigated in respect to personal data, including but not limited to payment card information, or privacy practices? c) Been asked to supply any regulator or similar body with information relating to personally identifiable information or privacy practices? d) Received any complain relating to the handling of someone’s personally identifiable information? e) Received any actual or attempted extortion demand with respect to its data or computer system? 	<ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <p>Please provide details on a separate page.</p>

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.

6.2	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 Please provide details on a separate page.
If you have answered no to any of the above, please provide additional information.		

7.0 Declaration**You further confirm and agree that:**

By entering your name and email, you agree that all information provided to BOXX Insurance to generate this insurance policy is accurate and true.

You consent to BOXX Insurance Inc. using the information we may hold about you for the purpose of providing insurance and handling claims, if any, and to process sensitive personal data about you where this is necessary. This may mean we have to give some details to third parties involved in providing insurance cover.

The information provided will be treated in confidence and in compliance with relevant Data Protection legislation. You have the right to apply for a copy of your information (for which we may charge a small fee) and to have any inaccuracies corrected.

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.

Your Name & Title:		
Signature:		
Email:		Dated:

Extra Notes Page

--