cyberboxx	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; Broadcaster; Film production/publishers; Franchisees/Franchisor ☐Yes ☐No		

Create your preferred Cyberboxx option:

Select Coverage Limit:	$250,000, $500,000, $1,000,000, $2,000,000 or $3,000,000	Please select from the drop-down list:	$3,000,000
Add Cyber Crime & Fraud Sub Limit	$100,000 or $250,000	Please select from the drop-down list:	$250,000
Select Deductible	$10,000, $25,000, $50,000, $100,000	Please select from the drop-down list:	$100,000

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:	>2,000,000
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. a) Names, addresses and email addresses b) Individual taxpayer ID/ social security numbers / driving licenses / passport information c) Financial account records / payment card data d) Healthcare information	☐Yes ☐No ☐Yes ☐No ☐Yes ☐No ☐Yes ☐No

cyberboxx	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.

1.3	Have you conducted a review to determine what personal data you handle and where it is stored?	☐Yes ☐ No
1.4	Do you encrypt personal data: a) at rest? b) in transit? c) on corporate laptops? d) on removable media? e) on mobile devices? f) on backups?	☐Yes ☐ No ☐Yes ☐No ☐Yes ☐No ☐Yes ☐ No ☐Yes ☐No ☐Yes ☐No
1.5	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?	☐Yes ☐No ☐Yes ☐No
1.6	Do you obtain explicit consent from customers when collecting personal data?	☐Yes ☐ No
1.7	Do you maintain a written policy that addresses information security which is communicated to all employees?	☐Yes ☐ No
1.8	Do you mandate information security training for staff that have access to your information resources on at least an annual basis?	☐ Yes ☐ N
1.9	If you use third parties to host your data, do they comply with any information security frameworks or information management schemes?	☐ Yes ☐ No
1.10	Do you have a written privacy policy that has been reviewed by a suitably qualified lawyer?	☐ Yes ☐ No
1.11	Do you accept credit card payments in your facilities or via the web? If yes, please answer the following questions: • 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?	☐Yes ☐ No ☐Yes ☐ No ☐Yes ☐ No

2.0 Security Controls & Network Governance		
2.1	Is there an individual in your organization specifically assigned responsibility for information security such as a CISO?	☐ Yes ☐ 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?	☐ Yes ☐ No ☐Yes ☐ No
2.3	Have you installed and do you maintain firewall configuration to protect your data and network?	☐ Yes ☐ No
2.4	How frequently are software patches applied (including mission-critical or revenue-generating systems)? Please select from the drop-down list:	90 days+
2.5	Have you installed physical controls to protect sensitive systems and sensitive physical information under your care, custody, or control?	☐Yes ☐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 organization?	☐Yes ☐ No
2.7	Do you have a process for user account creation, approval and removal?	☐Yes ☐ No
	If you have answered no to any of the above, please provide additional information.	

3.0 Ransomware Protection		
3.1	Do you employ an email monitoring solution (e.g. ProofPoint)?	☐Yes ☐No
3.2	Have you implemented Sender Policy Framework (SPF), DKIM or DMARC email security solutions?	☐Yes ☐ No
3.3	Do you have the capability to inspect, sandbox and block suspicious email content and attachments?	☐Yes ☐ No
3.4	Do you restrict access to all sensitive information stored by you on a need to-to-know basis?	☐Yes ☐No

cyberboxx	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.

3.5	Do you change any default administrative passwords to an alternative that is difficult to guess?	☐Yes ☐No
3.6	Do privileged users have a separate administrative account in order to carry out specific administrative duties?	☐Yes ☐No
3.7	Do you have established processes for rapidly applying critical security patches across servers, laptops, desktops, and managed mobile devices?	☐Yes ☐No
3.8	Do you deploy non-critical patches across servers, laptops, desktops, and managed mobile devices within 30 days, and critical patches (CVSS v3 score of 7 or above) within 14 days frequently?	☐Yes ☐No
3.9	Do you rely on any operating systems, software, firmware or hardware that is no longer supported or is considered "end-of-life" (EOL) by the manufacturers? If yes: a. are these segmented from the rest of the network? b. are plans in place to remediate, upgrade and/or decommission?	☐Yes ☐No ☐Yes ☐No ☐Yes ☐No
3.10	The applicant confirms that multi-factor authentication is always enabled on emails and remote access. Please select from the drop-down list:	☐Yes ☐No
3.11	Does the organisation undertake phishing simulations on all employees?	☐Yes ☐No
3.12	Does your employee cyber security awareness program include phishing training and testing?	Annual Training ☐Yes ☐No Phishing Testing ☐Yes ☐No
3.13	Do you enforce password complexity requirements with a minimum password length of 12 characters?	☐Yes ☐No
3.14	Are all computer devices protected by anti-virus or endpoint protection software?	☐Yes (Endpoint) ☐Yes (AV) ☐No
3.15	Are your backups stored in a segregated environment, cloud environment or offline (e.g. backup tape)?	☐Yes ☐No
3.16	Are all endpoints protected by Endpoint Detection and Response software?	☐Yes ☐No
3.17	Do you ensure that only the necessary open ports are exposed to the internet?	☐Yes ☐No
3.18	Is remote desktop protocol (RDP) disabled? If 'no': a. is this limited to VPN access only, subject to multi factor authentication? b. If 'no' is network level authentication enabled?	☐Yes ☐No ☐Yes ☐No ☐Yes ☐No
3.19	Do you take backups of critical systems and data at least weekly?	☐Yes ☐No
3.20	Do your backups include backups of applications, databases, servers, workstations / laptops and endpoints?	☐Yes ☐No
3.21	Do you store your backups in an encrypted format?	☐Yes ☐No
3.22	Do you regularly test your ability to restore from backups?	☐Yes ☐No
	If you have answered no to any of the above, please provide additional information.	

cyberboxx	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.

4. 0	Business Interruption	
4.1	Do you maintain redundant back-ups of sensitive and critical system information?	☐ Yes (Offsite) ☐ Yes (Onsite) ☐ No
4.2	Are restore procedures documented and tested?	☐ Yes ☐ No
4.3	Do you use credentials unique to backups that are stored separately from other user credentials?	☐ Yes ☐ 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?	☐ Yes ☐ No ☐ N/A
4.5	Do you have protocols for replacement of end-of-life system/network equipment?	☐ Yes ☐ No
4.6	Are your critical information/SCADA equipment, segregated from the wider IT environment with internal firewalls and software protection?	☐ Yes ☐ No
4.7	Are any of these critical systems connected to the Internet?	☐ Yes ☐ No
4.8	Do you segregate your network by geography, to isolate any potential malware infections?	☐ Yes ☐ No
4.9	If so, how quickly can you obtain back-ups stored by third parties?	☐ 24 hours ☐ One week ☐ One month ☐ 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 ☐ DRP ☐ IRP ☐
	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?	☐ Yes ☐ No
5.2	Has specific financial crime training been provided to anyone who has authority to make payments greater than $2,000?	☐ Yes ☐ No
5.3	Do you require two parties to sign off on any payment transfers greater than $2,000?	☐ Yes ☐ No
5.4	Do you have policy in place to verify any changes to existing invoices, bank deposit information and contact information?	☐ Yes ☐ No
5.5	Before processing a wire transfer of funds OR changing vendor account details, do you confirm the request by a secondary means of communication in order to verify the instructions are legitimate?	☐ Yes ☐ No
	If you have answered no to any of the above, please provide additional information.	

6.0 Prior Claims		
6.1	**Prior Claims: During the past 5 years, have you:** 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?	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No Please provide details on a separate page.

cyberboxx	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.

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?	☐Yes ☐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