

Cyber Application

SECTION A - GENERAL INFORMATION

Company Name (include any subsidiaries to be listed on the policy):

Primary Business Activity:

Operating Countries:

Website:

Revenue (from last complete financial year):

SECTION B - NETWORK SECURITY AND DATA MANAGEMENT

1.	Is your organization compliant with all applicable cyber, privacy, and data protection legislation and regulations?	Yes	No
2.	Do you have anti-virus or industry recognised endpoint protection solution on all endpoints across your network?	Yes	No
3.	In what time frame do you install critical software security patches?		
4.	Do you utilize any un-supported end-of-life operating systems (e.g. Windows 7, Windows XP)?	Yes	No
5.	Do you maintain physically disconnected ('offline') back-ups for all critical data (e.g. tape drives)?	Yes	No
	<i>a) How frequently are offline back-ups taken?</i>		
	<i>b) Are these backups immutable and/or air-gapped?</i>		
6.	Do you require the use of two-factor authentication for all remote network access?	Yes	No
7.	Do you require the use of two-factor authentication for all webmail access (e.g. Office365)?	Yes	No
8.	Do you utilize behavioural analysis and/or machine learning endpoint detection and response (EDR) or MDR software to detect malware for which no anti-virus signatures exist?	Yes	No
	<i>If Yes, please state the software product used (e.g. Sentinel One, CrowdStrike Falcon):</i>		
9.	With respect to personal or sensitive data (e.g. customer PII or PHI) stored on your networks:		
	<i>a) Is the data encrypted at rest?</i>		
	<i>b) Do you encrypt all mobile devices and laptops which are used to store personal data?</i>	Yes	No
10.	Do all employees receive training on phishing and other social engineering techniques?	Yes	No
11.	Do you accept credit card payments for any of your goods or services rendered?	Yes	No
	<i>a) If yes, do all your point-of-sale systems have end-to-end encryption (E2EE) or point-to-point (P2PE) deployed (or this is in place through your outsourced card payment provider).</i>	Yes	No
12.	Do you have a review process to screen content and matter disseminated via your website and social media channels?	Yes	No



SECTION C - LIMITS					
\$25,000	\$50,000	\$100,000	\$250,000	\$500,000	\$1,000,000

SECTION D – OPTIONAL CYBERCRIME SUBLIMIT		
1. Prior to transferring funds to new accounts or changing existing account details, is the request verified using an authentication method different from the one used to submit the request?	Yes	No
2. Are electronic fund transfers and cheques over \$25,000 subject to dual review and authorization by at least two staff members?	Yes	No
Cybercrime Limit		
\$25,000	\$50,000	\$100,000

SECTION E - CLAIMS / CIRCUMSTANCES	
1. Have you had any claims or circumstances within the past 5 years that would have triggered the proposed policy?	
a) If yes, please describe the incident(s) and total costs:	
b) Considering any incident please provide details of any repeat attacks and remediation work that has been undertaken as a result.	

I declare that after proper inquiry the statements and particulars given above are true and that I have not mis-stated or suppressed any material fact.

I agree that this proposal form, together with any other material information supplied by me shall form the basis of any contract of insurance affected thereon.

I undertake to inform underwriters of any material alteration to these facts occurring before the completion of the contract.

Signed:

Date:

Name:

Title: