Cyber Insurance Proposal Form

For Applicants with Revenue Below NZD 250m

QBE Insurance (Australia) Limited ABN 78 003 191 035 AFSL 239 545

Notice to the Applicant

You must read this notice before you complete this Proposal Form.

Material facts

'You' (this includes every person or entity to be insured under this insurance) are under a duty to disclose all material facts that could influence QBE Insurance's decision to accept this insurance and, if so, on what terms. You need to disclose facts both known to you and those which you could have been reasonably expected to know about. If you are in any doubt as to whether or not a fact may be material, you should disclose it to ensure that any cover granted is not prejudiced.

Non-disclosure/misstatement

If you fail to comply with your duty of disclosure, QBE may be entitled to avoid the contract altogether, and therefore decline to pay any claim.

Jurisdiction

Except where the parties agree otherwise, the laws of New Zealand apply to this form and any dealings between the parties arising from this form. The New Zealand courts have exclusive jurisdiction in relation to any disputes that may arise.

How to complete this form

- You must answer all questions fully and, if you are completing this form by hand, please ensure you write clearly.
- If you are completing this form electronically, please open it using the latest version of Adobe Reader. Use your mouse/trackpad to take the cursor to the next editable field. Boxes can be ticked either by using your mouse/trackpad or by hitting 'enter'. Upon completion, please print out this form and sign the declaration.
- The signed form should then be posted, or emailed, to your broker.

General Applicant Information

Applicant Legal Name:				
NZBN:				
Address:				
	Country:		**Post Code:**	
Industry Sector:				
Business Description:				
Website Domain(s):				
No. of Employees:				

1. Are you a subsidiary, franchisee, or smaller entity of a larger organisation?

☐ Yes ☐ No *If Yes, please provide brief details:*

2. QBE provides a range of threat intelligence, event detection and complimentary cyber risk services to enhance cyber resilience. Please provide the point of contact at your organisation to receive updates and information on these services.

Name	Title
Email	**Phone No.**

Organisation and Financial Information

3. Revenue:	Prior Financial Year	Current Financial Year	Next Financial Year
Total Revenue:			
% US Revenue:			
% Other Overseas Revenue:			

(if Overseas (OS) flagged, please provide separately any available subsidiary list or organisational chart)

4. Will there be any significant change to the nature or size of your business in the next 12 months, including but not limited to a merger, acquisition, or consolidation? ☐ Yes ☐ No

If Yes, please provide brief details:

5. Are you engaged in any of the following activities?

Cultivation, manufacturing, sale, or distribution of any cannabis products. ☐ Yes ☐ No

Non-fungible tokens (NFTs), cryptocurrency, or blockchain technology. ☐ Yes ☐ No

Adult content or gambling. ☐ Yes ☐ No

Managed Service Provider (MSP), or Managed Security Service Provider (MSSP). ☐ Yes ☐ No

6. Please indicate the approximate number of individual records you store for each of the following categories:

Personally Identifiable Information (PII)	Protected Health Information (PHI)	Payment Card Information (PCI)	Biometric Data

Cybersecurity and Privacy Controls

7. Is Multi-Factor Authentication (MFA) required for all forms of remote access to your systems, including but not limited to VPN, RDP, and cloud services? ☐ Yes ☐ No

8. Is Multi-Factor Authentication (MFA) required for access to web-based email? ☐ Yes ☐ No ☐ *No web-based email permitted*

9. Do you conduct organisation-wide awareness campaigns for social engineering (such as phishing, vishing, and smishing) at least once a year? ☐ Yes ☐ No

10. Which of the following email security controls do you have in place? Please select all that apply:

- ☐ Tagging of external emails
- ☐ Email Data Loss Prevention (DLP) solutions
- ☐ Malware scanning for malicious links and attachments
- ☐ Email quarantine service implemented
- ☐ Email sandboxing solution implemented
- ☐ Implementation of one or all these email protocols: DMARC, DKIM, and SPF

11. Which types of security software solutions have you implemented? Please select all that apply and specify vendor and percentage of devices protected:

	Product Name	% Coverage
Anti-malware and anti-virus software		
Endpoint Protection Platform (EPP)		
Endpoint Detection and Response (EDR)		
Managed Detection and Response (MDR)		
Extended Detection and Response (XDR)		
Managed Extended Detection and Response (MXDR)		

12. Do you have an established policy for managing and installing critical patches for systems exposed to the internet? ☐ Yes ☐ No

13. How frequently do you take backups of critical systems and data?

☐ Daily or weekly ☐ Monthly ☐ Quarterly ☐ Never or not regularly

Cybersecurity Questions ONLY for Applicants with Revenue Above 100m

14. Do you have a policy to disable macros by default in office documents and email attachments? ☐ Yes ☐ No

15. Do you have an Advanced Threat Protection (ATP) solution in place to safeguard your email systems against threats such as phishing, malware, and business email compromise? Some examples are Microsoft 365 Defender ATP, Mimecast, and Proofpoint. ☐ Yes ☐ No

16. Within what timeframe does your organisation typically implement critical patches? A critical patch is one with CVSS score of 9.0 or higher .

☐ 0-24 hours ☐ Less than one week ☐ More than a month
☐ 24-48 hours ☐ Less than one month

17. Do you have a Security Operations Centre (SOC) in place? If yes, is your SOC managed internally or is it outsourced to a Managed Security Services Provider (MSSP)?

☐ Yes, 24/7 ☐ No ☐ Internal
☐ Yes, working hours ☐ Outsourced ☐ Both outsourced and internal

18. Do you have a documented incident response plan in place that includes triage, escalation and response processes for security incidents, data privacy events and system outage events? ☐ Yes ☐ No

19. Do you have a business continuity plan that takes into account the recovery and restoration of critical systems (i.e. disaster recovery processes) during a cyber incident? ☐ Yes ☐ No

20. Are your backups segmented from your main network and secured with separate credentials accessible only to privileged users? ☐ Yes ☐ No ☐ *No, but we use immutable backups*

Funds Transfer Controls

21. Do you have a formal, documented process for verifying the legitimacy of wire transfer requests, especially when there are changes to existing vendor information or for transactions above a certain threshold? ☐ Yes ☐ No

22. Do you conduct mandatory social engineering and anti-fraud training for all employees who are responsible for disbursing or transmitting funds? ☐ Yes ☐ No

23. Is there a multi-step approval process in place for wire transfers, including segregation of duties and additional verification for transfers above a specified amount? ☐ Yes ☐ No

Media Content Controls

24. Do you have a process to review all content prior to posting on your website, intranet or social media pages? ☐ Yes ☐ No

If Yes, does the review include screening the content for the following:

☐ Disparagement issues
☐ Unauthorised use of name, likeness, and identity
☐ Unlicensed music
☐ Copyright infringement
☐ Invasion of privacy

If Yes, is the review performed by a qualified attorney or by someone who receives regular training in each of the above categories? ☐ Yes ☐ No

25. Have you performed a search and review of all past audio-visual web or social media posts to ensure music synchronisation licenses were obtained, or that posts where proof of such license could not be confirmed have been removed? ☐ Yes ☐ No

26. Do you have a procedure for responding to allegations that content created, displayed, or published by the Applicant is defamatory, infringing, or in violation of a third party's privacy rights (including name, likeness, and identity)? ☐ Yes ☐ No

27. Do you have a formal takedown procedure in place for removing media content that is potentially defamatory, infringing on copyright or trademark, or violating intellectual property rights? ☐ Yes ☐ No

Additional Details

28. Please include additional details to clarify any of your answers.

Prior Claims and Circumstances

29. Do you have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim or loss or obligation to provide breach notification under the proposed insurance? ☐ Yes ☐ No

If Yes, please provide details:

30. During the past five (5) years, has the Applicant:

a. Received any claims or complaints with respect to privacy, breach of information or network security, unauthorised disclosure of information, defamation, or content infringement? ☐ Yes ☐ No

b. Been subject to any government action investigation or subpoena regarding any alleged violation of a privacy law or regulation? ☐ Yes ☐ No

c. Notified consumer or any other third party of a data breach incident involving the Applicant? ☐ Yes ☐ No

d. Experienced an actual or attempted extortion demand with respect to its computer systems? ☐ Yes ☐ No

e. Has a director or an officer of the Applicant ever had proceedings (civil or criminal) initiated against them alleging misconduct or breaches of the law in their capacity as a director or officer of a company? ☐ Yes ☐ No

f. In the last five (5) years has the Applicant suffered any loss exceeding $5,000 as a result of fraud or dishonesty committed by an employee? ☐ Yes ☐ No

If Yes to any of the above questions, please provide details of any such action, notification, investigation, or subpoena:

Declaration and Signature

I/We declare, on behalf of all proposed insureds, that:

(a) All answers and statements in this proposal are correct and complete in every respect and there is no further information which may affect acceptance of the proposal.

(b) If accepted by QBE, this proposal and declaration, and any other material which I/we have provided to QBE, shall be incorporated into and form the basis of the contract of insurance.

(c) I/We warrant that I/We will notify QBE of any material alteration to these facts whether occurring before or after the completion of this proposal.

(d) If any personal information is provided, I/We understand that:

  (i) This information will be collected, held, used and disclosed by QBE (either in New Zealand or overseas) in order to issue, administer and manage products and provide services, including claims investigation and administration, and for data analytics. Further details are set out in QBE's privacy policy available at https://www.qbe.com/nz/about-qbe/privacy-and-your-personal-information.

  (ii) If I/We do not provide the information requested, then QBE may be unable to provide products or services.

  (iii) Where I/We have provided someone else's personal information, I/We confirm that I/We have obtained their consent to do so.

(e) QBE is authorised to disclose information received from me/us to its advisers, reinsurers and to other insurers. I/We authorise QBE to obtain, from any party, information that is, in QBE's view, relevant to this proposal.

(f) I/We understand that the insurance will not be in force until this proposal has been accepted and cover confirmed by QBE.

Note: Signing this proposal and any supplementary questionnaires does not bind either the applicant or QBE to complete the contract of insurance.

Signature of applicant's authorised representative	Date

Printed name of signatory	Company name	Title

E-mail address	Phone number