RAHEJA
QBE

Raheja QBE CyberProtect Insurance Policy – Proposal form

NOTICE: THE POLICY FOR WHICH THIS APPLICATION IS BEING SUBMITTED IS WRITTEN ON A CLAIMS MADE AND REPORTED BASIS. THE POLICY ONLY COVERS CLAIMS FIRST MADE AGAINST THE INSUREDS DURING THE POLICY PERIOD AND REPORTED IN WRITING TO THE INSURER PURSUANT TO THE TERMS THEREIN. THE LIMIT OF LIABILITY AVAILABLE TO PAY LOSSES WILL BE REDUCED AND MAY BE EXHAUSTED BY DEFENSE EXPENSES. DEFENSE EXPENSES WILL BE APPLIED AGAINST THE RETENTION AMOUNT.

Instructions: This form must be dated and signed by the CEO, President, CFO, Risk Manager, General Counsel or other officer acceptable to RQBE. Applicant means all corporations, organization or other entities, including subsidiaries, proposed for this insurance coverage.

General Applicant Information

Applicant Legal Name:

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 organization? Yes ☐ No ☐

   If Yes, please provide brief details:

2. RQBE 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 organization to receive updates and information on these services.

Name	Title	Email	Phone No.

Organization and Financial Information

3. Revenue:

	Prior Financial Year	Current Financial Year	Next Financial Year
Total Revenue:			
% US Revenue:			

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 have controls to prevent general users from having local administrator rights on corporate devices? Yes ☐ No ☐

10. Do you require Multi-Factor Authentication (MFA) for privileged user access, including Domain Administrators, to Azure Active Directory (AAD)? Yes ☐ No ☐ Not applicable, we do not use AAD ☐

11. How many active Domain Administrator accounts exist within your organization?

12. What specific controls do you have in place to safeguard Domain Administrator accounts?

Please select all that apply:

- ☐ Separate administrative accounts from standard user accounts
- ☐ Multi-Factor Authentication (MFA) required for access, where possible
- ☐ Credentials are rotated at least monthly or upon use
- ☐ Passwords of at least 25 characters in length
- ☐ Access is recorded and audited
- ☐ Tiered model implemented to separate domain-wide admin accounts from workstation or server management ones
- ☐ Prohibited from running services or applications
- ☐ Domain administrators prohibited from accessing the internet
- ☐ Access restricted to specific workstations
- ☐ Privileged Access Management (PAM) solution implemented to control access

13. Are firewall configurations set to default deny (reject all traffic unless explicitly allowed) and updated at a minimum on an annual basis? Yes ☐ No ☐

14. Do you maintain an up-to-date inventory of all your hardware and software assets exposed to external networks? If yes, please specify percentage of assets covered by inventory.

Yes ☐ % No ☐

15. If you have any end-of-life (EOL) systems in your network, do you employ one or more of the following controls? 1) Purchase of extended support where available, 2) segmentation from the rest of the network, and/or 3) isolation from the internet.

Yes ☐ No ☐ No EOL systems in use ☐

16. Do you use baseline system configurations or hardened images to securely configure your operating systems in alignment with industry best practices (e.g., CIS or NIST benchmarks)?

If yes, please specify percentage of assets this applies to: Yes ☐ % No ☐

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

If Yes, are click rates monitored and campaigns adjusted to be more effective when appropriate?

Yes ☐ No ☐

18. 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

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

20. 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 ☐

21. 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)		

22. Do you conduct regular vulnerability scans of your systems and networks? Yes ☐ No ☐

If Yes, please specify type of scan and frequency.

External		Internal	
Continuously	%	Continuously	%
Daily	%	Daily	%
Weekly	%	Weekly	%
Monthly	%	Monthly	%
Quarterly	%	Quarterly	%
Ad hoc	%	Ad hoc	%

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

24. Within what timeframe does your organization 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 one month
☐ 24-48 hours ☐ Less than one month

25. Do you have a Security Operations Center (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

26. 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 ☐

27. Do you conduct incident response tabletop exercises that include technical, operational and leadership teams at least once per year? Yes ☐ No ☐

28. 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 ☐

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

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

30. Are your backups segmented from your main network and secured with separate credentials accessible only to privileged users?

Yes ☐ No, but we use immutable backups ☐ No ☐

31. How frequently do you conduct restoration tests to ensure backup effectiveness?

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

PCI Controls

Please complete this section if you process, store, or transmit credit card information, and/or if you are subject to Payment Card Industry Data Security Standards (PCI DSS). Otherwise, please confirm this is not applicable to you: N/A ☐

32. Do you store any cardholder data (such as full credit card numbers, CVV codes, or PIN numbers) in your network in any form, including databases, log files, or backups? Yes ☐ No ☐

33. Do you implement end-to-end encryption (E2EE), point-to-point encryption (P2PE), or tokenization for all payment card transactions and data transmissions? Yes ☐ No ☐

34. Are your point-of-sale (POS) terminals EMV (chip-and-PIN) compliant? Yes ☐ No ☐

Funds Transfer Controls

35. 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 ☐

26. 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 ☐

27. Do you conduct incident response tabletop exercises that include technical, operational and leadership teams at least once per year?
Yes ☐ No ☐

28. 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 ☐

29. How frequently do you take backups of critical systems and data?
☐ Daily or weekly ☐ Quarterly
☐ Monthly ☐ Never or not regularly

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

31. How frequently do you conduct restoration tests to ensure backup effectiveness?
☐ Daily or weekly ☐ Quarterly ☐ Never or not regularly
☐ Monthly ☐ Annually

PCI Controls

Please complete this section if you process, store, or transmit credit card information, and/or if you are subject to Payment Card Industry Data Security Standards (PCI DSS). Otherwise, please confirm this is not applicable to you: N/A ☐

32. Do you store any cardholder data (such as full credit card numbers, CVV codes, or PIN numbers) in your network in any form, including databases, log files, or backups?
Yes ☐ No ☐

33. Do you implement end-to-end encryption (E2EE), point-to-point encryption (P2PE), or tokenization for all payment card transactions and data transmissions?
Yes ☐ No ☐

34. Are your point-of-sale (POS) terminals EMV (chip-and-PIN) compliant?
Yes ☐ No ☐

Funds Transfer Controls

35. 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 ☐

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

37. 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 ☐

Operational Technology Controls

Please complete this section if you rely on Operational Technology (OT) for your business's mission critical processes, or if you are in the manufacturing, energy, utilities, and/or transportation industries. Otherwise, please confirm this is not applicable to you: N/A ☐

38. Is Multi-Factor Authentication (MFA) required for remote access to your Operational Technology (OT) environment for both employees and third-party individuals?

Yes (both) ☐ Yes (employees only) ☐ No ☐ Remote access not permitted ☐

39. Are all OT environments segmented from all IT environments? Yes ☐ No ☐

40. Do you manage the credentials and maintain logs for OT users independently from those of IT users? Yes ☐ No ☐

41. Are all OT environments disconnected from the internet? Yes ☐ No ☐

42. Does your business continuity plan include system outage restoration and recovery processes for OT systems? Yes ☐ No ☐

Media Content Controls

43. 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
☐ copyright infringement
☐ unlicensed music
☐ unauthorized use of name, likeness, and identity
☐ 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 ☐

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

45. 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 ☐

46. 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

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

Prior Claims and Circumstances

48. 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:

49. 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, unauthorized 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 ☐

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

Declaration and Signature

This application is not a representation that coverage does or does not exist for a particular claim, suit or loss, or type of claim, suit or loss, under any insurance policy issued by the insurer. Whether coverage exists or does not exist for a particular claim, suit or loss under such policy depends on the facts and circumstances involved in the claim, suit or loss and all applicable policy wording. If a policy is issued, this application will be attached to and made a part of the policy.

The undersigned authorized representative of Applicant declares and certifies that all statements set forth in this application and attachments hereto are true, correct and complete, and that no material facts have been misstated or misrepresented in this application, omitted or concealed.

Signing this application shall not constitute a binder or obligate the insurer to provide coverage, but it is agreed that this application (together with any attachments hereto) is and will continue to be relied upon should a policy be issued.

Signature of applicant's authorized representative

Printed name

Company name

Title

E-mail address

Phone number

INSURANCE ACT 1938, SECTION 41 - PROHIBITION OF REBATES

No person shall allow or offer to allow, either directly or indirectly as an inducement to any person to take out renew or continue an insurance in respect of any kind of risks relating to lives or property in India, any rebate of the whole or part of the commission payable or any rebate of the premium shown on the policy, nor shall any person taking our or renewing or continuing a Policy accept any rebate, except such rebate as may be allowed in accordance with the published prospectus or tables of the insurer.

Any person making default in complying with the provisions of this section shall be punishable with fine which may extend to ten lacs rupees.

DECLARATION FOR COMPLIANCE WITH ANTI-MONEY LAUNDERING REGULATIONS

We_____(Insured Named) hereby declare that the source of funds for the premium paid for obtaining this insurance cover is through legitimate funds from our Bank Account No. _____with _____ _____.(Name of the Bank)_____ (Bank Branch & IFSC Code).

Place & Date: …….. Signature & Stamp of the Insured……

Please provide copy of a cancelled cheque if premium is paid through NEFT /ECS /RTGS

Please enclose one document of 'Proof of Identity' and one document as 'Proof of Address' with this application.

The following documents are accepted as:

Proof of Identity:	**Proof of Address:**
For Individuals	
1. Passport 2. PAN Card 3. Driver's License 4. Voter's Identity Card 5. Letter from Recognized Public Authority	1. Telephone/Mobile bill not older than six months on the date of commencement of insurance 2. Bank A/c Statement with Residential address not older than six months on the date of commencement 3. Electricity Bill 4. Ration Card 5. Valid Lease Agreement along with Rent Receipt for 3 Months preceding the date of commencement of risk 6. Employer's Certificate 7. Letter from Recognized Public Authority
For Companies	
1. Certificate of Incorporation and Memorandum and Articles of Association. 2. Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account. 3. Power of Attorney granted to its managers, officers or employees to transact business on its behalf. 4. Copy of PAN allotment letter	
For Partnership Firms	
1. Registration Certificate 2. Partnership Deed 3. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf. 4. An officially valid document identifying the partners and the persons holding the Power of Attorney and their address.	
For Trusts and Foundations	
1. Certificate of registration, if registered. 2. Power of Attorney granted to transact business on its behalf. 3. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their address. 4. Resolution of the founding body of the foundation/trust/association.	

Please note that this is not an exhaustive list. If you do not have any of these documents please contact your Agent/Broker/ nearest Raheja QBE Office or call our Toll Free Number 1800 - 102 - 772