

# Cyber and Data Security proposal form

Please read the proposal form carefully and fill in

- a) All sections in capitals and tick boxes wherever applicable.
- b) Failure to disclose facts material to the assessment of the risk or providing misleading information may render the contract VOID.
- c) Attach separate sheets if space given is insufficient

## Your business

Name(s) in full of all entities to be insured


Websites

www.
www.
www.
www.

Please list the locations from which you conduct business including overseas domiciled locations:


Commencement date of your business     /     /

Please provide the following details in respect of your principals or directors:

Name	Qualifications	Year qualified	Years practicing as principal	
			This firm	Previous firm
		/ /		
		/ /		
		/ /		
		/ /		

## Business details

Please detail the sector in which your business operates and describe the operations performed by your business.

Please supply total numbers

of	
Partners/principals/directors	
Professional staff	
Consultants	
System analysts / designers	

Programmers	
Sales & marketing	
Administration / supports	
Other (please specify)	

Total	
-------	--

In the past five(5) years

- |  |     |    |
|--|-----|----|
| (a) Has the name of the business changed?  | Yes | No |
| (b) Have you purchased or merged with any other business?  | Yes | No |
| (c) Have you sold or demerged from any other business?   | Yes | No |
| (d) Do you require cover for any subsidiary, joint venture or associated company?  | Yes | No |
| (e) Do you expect any significant change to your operations or the development and release of new services /products over the next twelve (12) months? | Yes | No |

If 'yes' to any of the above, please supply details:

## Financial details

Please supply details of your total revenue (include fee income, net profit/loss (before tax), gross wage roll) from the countries in which you conduct business:

Country	Currency	Revenue last financial year	Revenue current financial year (forecast)	Revenue next financial year (forecast)
Total			0	0

Please provide the percentage of total gross revenue that is assigned to the IT budget:

Please provide the percentage of gross revenue derived from e-commerce:

Please state the approximate percentage of your activities (based on revenue current financial year-forecast) applicable to each region:

India	Australia	USA/Canada	Europe	Rest of the world	Total
%	%	%	%	%	0 %

## IT operations

Which management positions are assigned within your organisation? (Please tick where appropriate)

Chief information officer	<input type="checkbox"/>	IT director	<input type="checkbox"/>	IT manager	<input type="checkbox"/>
Chief risk officer	<input type="checkbox"/>	IT/information security manager	<input type="checkbox"/>	Chief information security officer	<input type="checkbox"/>
Chief privacy officer	<input type="checkbox"/>	Chief compliance officer	<input type="checkbox"/>	Other/additional	<input type="checkbox"/>

Please provide numbers of:

Computer users:  Servers:  PC's:  Portables (laptops, smart phones etc):  Physical server locations:

Please confirm which (if any) of your IT functions are outsourced:

	In-house	Partially outsourced	Totally outsourced	To what level are you indemnified by the outsourcer?	Outsourcing vendor (please provide names)
IT services support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Infrastructure -telecoms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Infrastructure - network	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Business applications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Website hosting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
Other	<input type="checkbox"/>				

## IT operations(continued)

Please detail your risk management of third-party IT vendors (please tick where appropriate)

	Always undertaken	Ad-hoc basis	Never undertaken
Data security due diligence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Audits performed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contract requires security incident to be reported to you	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Controls

Do you have a governance framework/policy supporting a consistent and structured approach to information security?  Yes  No

Are all staff regularly updated on security best practice and the latest applicable privacy,data and security legislation?  Yes  No

Please detail your training processes for staff in respect of potential cyber threats and fraud:

Have you conducted a vulnerability scan and/or penetration test in the last 12months?(If any area of concern were highlighted ,please detail how these were/are to be addressed):

Do you carry out background screening on:

	Yes	No	Working towards
Staff with access to personally identifiable information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Staff with privileged systems access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please provide further details in the box below:

Please detail the checks for the authorisation of payments above INR 100,000 to third-parties:

## Controls(continued)

Please provide details of your system controls:

- (a) Are there restrictions on staff's ability to download and install software?  Yes  No
- (b) Are there restrictions on staff's access to confidential data dependent on their position in your company?  Yes  No
- (c) Is a central risk log in place for all cyber-incidents?  Yes  No
- (d) Does your system have anti-malware, firewall protection and automatic virus scans of computer systems?  Yes  No
- (e) Do you undertake regular intrusion detection and user activity monitoring?  Yes  No
- (f) Do you monitor networks in real-time for possible intrusions or abnormalities?  Yes  No

If 'no' to any of the above, please provide details:

## Business impact

If a business critical cyber-incident were to occur(a hacking event preventing the use of critical business systems for example),how long would it be before you were to suffer a loss of net profit?

- 48hours+       Between 24-48hours       Between 12-24 hours       Between 1-12hours       < 1 hour

How much net profit per day would you expect to lose if such a cyber-incident were to occur?

Do you employ the following (for the purposes of network interruption/privacy breach):

- (a) An incident response plan or disaster recovery plan  Yes  No
- (b) A business continuity plan  Yes  No
- If yes,has either of these plans been tested in the last 12months?  Yes  No
- (c) A manual work around to mitigate loss in the event of network outage?  Yes  No
- (d) Daily backup of sensitive data  Yes  No
- If yes, are backups stored in an off-site location?  Yes  No
- (e) Fail-over to a "hotsite" in the event your main hosting site goes down (owned or third party)  Yes  No

What is your expected recovery time after suffering a cyber-incident or experiencing down time of critical business systems?

- 48hours+       Between 24-48hours       Between 12-24 hours       Between 1-12hours       Immediately

Please detail your deletion/destruction procedures for data including limits on time held on systems:

Please provide details of your patching policy including testing and the ability to roll back to previous versions:

## Use, storage and protection of personal data

Please provide details of personal data stored and/or processed in the table below (please note that employee records should be separately outlined in the final row of the table):

	Stored on system *Including cloud storage (please answer yes/no)		Number of records stored	Processed annually (please answer yes/no)		Number of records processed	Are these records encrypted?	
Basic information (names, addresses etc)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Government document numbers (drivers licence number, passport number etc)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Financial account information (account numbers, sort-codes, credit/debit card numbers etc)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Health records	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Employee records including previous employees (if still held)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="text"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> No

What is the highest proportion of data stored in any one location?

Do you segregate critical data (financial account information, health records etc.) in an isolated environment?

Do you sell/share confidential data (including PII) to/with third-parties (please tick)?

Sell  Share

If so, is this expressly stated in the contracts/terms and conditions of those individuals whose data is sold or shared?

Yes  No

Where confidential data is sold and/or shared with a third-party, do they indemnify you for their authorized use of this information?

Yes  No

Do you store personally identifiable records in respect of US residents?

Yes  No

## Encryption and regulation

Please tick where appropriate to illustrate your encryption processes:

	Always encrypted	Sometimes encrypted	Never encrypted
Laptops, tablets & smart phones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Removable media (USB sticks, CD's etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mails and defined folders on the system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please detail encryption methods in place for confidential data, if none, please detail any processes in place to protect the data (e.g. encrypted or tokenised):

Please detail your level of compliance with the Payment Card Industry (PCI) data standards:

Level1  Level2  Level3  Level4  Noncompliant

Which other industry standards are you compliant with?

ISO27001

Other (please detail)

## Online communications

Please complete the table below outlining controls of online communications including social media and websites:

	Standard practice	Ad-hoc basis	Not practiced	N/A
User generated content monitored (including chat rooms, bulletins etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Permission from third parties to use their content	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Procedures in place to flag and remove inappropriate content	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Legal review of content published online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Do you operate any external facing platforms which are used by customers?

Yes  No

## Previous insurance

Do you currently purchase cyber

Yes  No

insurance? If YES, please confirm:

Name of insurer:

Renewal date:

Limit of indemnity:

Excess:

Premium:

Have you ever been refused this type of insurance, had special terms imposed by insurers or had a similar insurance cancelled?

Yes  No

If YES, please provide full details:

## Your insurance requirements

Cover	Currency	Limit of Indemnity	Excess/Deductible
Third party cover			
Section 1 - Cyber, data security and multimedia cover			
First party cover			
Section 2 - Data breach notification costs cover			
Section 3 - Information and communication asset rectification costs cover			
Section 4 - Regulatory defence and penalty costs cover			
Section 5 - Public relations costs cover			
Section 6 - Forensics costs cover			
Section 7 - Credit monitoring costs cover			
Section 8 - Cyber business interruption cover			
Section 9 - Cyber extortion cover			

## Claims & circumstances

Within the last 5 years have you sustained any systems intrusion, tampering, virus or malicious code attack, loss of data, loss of portable media, hacking incident, extortion attempts, data theft or similar?  Yes  No

Within the last 5 years have you received any claims or complaints with respect to allegations of invasion of or injury to privacy, identity theft, theft of information, breach of information security, content infringement or been required to provide notification to individuals due to an actual or suspected disclosure of personal information?  Yes  No

If 'Yes', please provide details:

Have you ever suffered a business outage that has lasted more than 6 hours?  Yes  No

If 'Yes', please provide details including date of claim and amounts paid or reserved by insurers and/or details of any business outages suffered

If 'Yes', what steps have been taken to prevent a reoccurrence:

Are there any potential claim(s) or circumstance(s) that are likely to give rise to a claim or loss against your company that would fall within the scope of this insurance?  Yes  No

If 'Yes', please provide details including estimated cost of claim/loss:

Have you been involved in any dispute or arbitration concerning products, services or intellectual property rights?  Yes  No

Have you sustained any loss from the suspected dishonesty or malice of any employee?  Yes  No

If 'Yes' to any of the above, please provide details below:

## Declaration

I the undersigned, after enquiry declare as follows:

1. I am authorized by each of the other entities to be insured to complete this proposal form.
2. I have read and understood the notice to the proposed insured at the back of the proposal form.
3. I have read this proposal form and the accompanying documents and acknowledge the contents of same to be true and complete.
4. I understand that, up until a contract of insurance is entered into, I am under a continuing obligation to immediately inform RQBE of any change in the particulars or statements contained in this proposal form or in the accompanying documents.

I hereby declare and warrant that to the best of my knowledge and belief the answers given above, documents or papers submitted, are complete in all respects and represent the true position and that I have not withheld any information material to this Proposal. I agree that this Proposal Form, the declarations and accompanying documents or papers shall form the basis of the contract proposed between me and the Company. Name of business

Signed: Partner, principal or director

Date

Rhaeja QBE General Insurance Company Limited  
5<sup>th</sup> Floor Winsor House Kalina CST Road Mumbai 400 098

**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 out 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:

<b>Proof of Identity:</b>	<b>Proof of Address:</b>
<b>For Individuals</b>	
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
<b>For Companies</b>	
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	
<b>For Partnership Firms</b>	
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.	
<b>For Trusts and Foundations</b>	
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