Cyber and Data Security proposal form

QBE Insurance (Malaysia) Berhad Reg. No.: 198701002415 (161086-D)

(Part of QBE Insurance Group)
(Licensed under the Financial Services Act 2013 and regulated by Bank Negara Malaysia)
No. 638, Level 6, Block B1, Leisure Commerce Square, No. 9, Jalan PJS 8/9, 46150 Petaling Jaya,
Postal Address P.O. Box 10637, 50720 Kuala Lumpur, Malaysia.
telephone +603 7861 8400 • facsimile +603 7873 7430
SST Reg No: B16-1808-31042744
www.qbe.com/my

IMPORTANT NOTICE

1. **Pursuant to Paragraph 5 of Schedule 9 of the Financial Services Act 2013:**
   a) **if you are applying for this Insurance wholly for yourself/family/dependants (Consumer Insurance Contract), you have a duty to take reasonable care not to make a misrepresentation in answering the questions in this Proposal Form. You must answer the questions in this Proposal Form fully and accurately. Failure to take reasonable care in answering the questions may result in avoidance of your contract of insurance, refusal or reduction of your claim(s), change of terms or termination of your contract of insurance.**

   b) **if you are applying for this Insurance for purposes related to your trade, business or profession (Non-consumer Insurance Contract), you have a duty to disclose any matter that you know to be relevant to our decision in accepting the risks and determining the rates and terms to be applied and any matter a reasonable person in the circumstances could be expected to know to be relevant, otherwise it may result in result in avoidance of your contract of insurance, refusal or reduction of your claim(s), change of terms or termination of your contract of insurance.**

   This duty of disclosure for Consumer and Non-Consumer Insurance Contract shall continue until the time the contract is entered into, varied or renewed.

2. **For all intents and purposes where there is a conflict or ambiguity as to the meaning in the Bahasa Malaysia provisions of any part of the Contract, it is hereby agreed that the English version of the Contract shall prevail.**

Cover Note No.		**Intermediary No.**	
Intermediary Contact Number		**Intermediary Name**	

Name of Company

(Hereinafter referred to as "Company" in this Proposal and in the Policy)

Principal Address

Postal Code		**Contact no**	

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	Years practicing as principal: Previous firm

Clear 1

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		**Programmers**	
Professional staff		**Sales & marketing**	
Consultants		**Administration / supports**	
System analysts / designers		**Other (please specify)**	
		Total	0

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	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:

Asia	Australia	USA/Canada	Europe	Rest of the world	Total
%	%	%	%	%	%

Clear 2

IT OPERATIONS

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

Chief information officer	☐	IT director	☐	IT manager	☐
Chief risk officer	☐	IT/information security manager	☐	Chief information security officer	☐
Chief privacy officer	☐	Chief compliance officer	☐	Other/additional	☐

Please provide numbers of:

Computer users: ☐ Servers: ☐ PC's: ☐ Portables (laptops, smartphones 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	☐	☐	☐		
Infrastructure - telecoms	☐	☐	☐		
Infrastructure - network	☐	☐	☐		
Business applications	☐	☐	☐		
Website hosting	☐	☐	☐		
Other	☐	☐	☐		

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

	Always undertaken	Ad-hoc basis	Never under taken
Data security due diligence	☐	☐	☐
Audits performed	☐	☐	☐
Contract requires securityincident to be reported to you	☐	☐	☐

Clear 3

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 12 months? (If any areas 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	☐	☐	☐
Staff with privileged systems access	☐	☐	☐

Please provide further details in the box below:

Please detail the checks for the authorisation of payments above US$3,000 to third-parties:

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:

Clear 4

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?

☐ 48 hours+ ☐ Between 24-48 hours ☐ Between 12-24 hours ☐ Between 1-12 hours ☐ <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 12 months?	☐ Yes	☐ No
(c)	A manual workaround 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 "hot site" 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 downtime of critical business systems?

☐ 48 hours+ ☐ Between 24-48 hours ☐ Between 12-24 hours ☐ Between 1-12 hours ☐ 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)	☐ Yes ☐ No		☐ Yes ☐ No		☐ Yes ☐ No
Government document numbers (drivers licence number, passport number etc)	☐ Yes ☐ No		☐ Yes ☐ No		☐ Yes ☐ No
Financial account information (account numbers, sort-codes, credit/ debit card numbers etc)	☐ Yes ☐ No		☐ Yes ☐ No		☐ Yes ☐ No
Health records	☐ Yes ☐ No		☐ Yes ☐ No		☐ Yes ☐ No
Employee records including previous employees (if still held)	☐ Yes ☐ No		☐ Yes ☐ No		☐ Yes ☐ No

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

Clear 5

USE, STORAGE AND PROTECTION OF PERSONAL DATA (Continuation)

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 unauthorised 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	☐	☐	☐
Removable media (USB sticks, CD's etc)	☐	☐	☐
E-mails and defined folders on the system	☐	☐	☐

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

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

Level 1	Level 2	Level 3	Level 4	Non compliant
☐	☐	☐	☐	☐

Which other industry standards are you compliant with?

ISO 27001	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)	☐	☐	☐	☐
Permission from third parties to use their content	☐	☐	☐	☐
Procedures in place to flag and remove inappropriate content	☐	☐	☐	☐
Legal review of content published online	☐	☐	☐	☐

Do you operate any external facing platforms which are used by customers?	☐	Yes	☐	No

PREVIOUS INSURANCE

Do you currently purchase cyber insurance?	☐	Yes	☐	No

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:

Clear 6

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:

Clear 7

DECLARATION AND SIGNATURE

Privacy Policy Statement

I/We understand, acknowledge, agree and consent that QBE Insurance (Malaysia) Berhad and all of its related companies ("QBE") is permitted to collect, use, disclose and/or process my personal data revealed hereto. QBE is at liberty to disclose and transfer (including outside Malaysia) such personal data to relevant third parties provided that the revelation of my personal data is strictly for the purpose(s) in relation to the insurance which I have applied hereto, including but not limited to, the purpose(s) of: (i)processing, handling and/or dealing with my claims including the settlement of the claims and any necessary investigations relating to the claims; (ii) exercising any rights that QBE may have to recover monies from third parties; (iii) making reinsurance recoveries; (iv) investigating the accident and/or my claims; (v) carrying out and/or dealing with my instructions or responding to any enquiries by me; (vi) administering my claims (including the mailing of correspondence, statements, invoices, reports or notices to me, which could involve disclosure of certain personal data about me to bring about delivery of the same as well as on the external cover of envelopes/mail packages); (vii) the development of databases on claims, claims statistics and/or claims development; and/or (viii) complying with applicable law in administering, processing, handling and/or dealing with my claims; (collectively the "Purpose"). My consent given hereto covers any repeated collection of my personal data in the same circumstances and is in line with the requirement set forth on the Personal Data Protection Act 2010.

QBE Insurance (Malaysia) Berhad is committed to ensuring the safety and security of your personal data. You may refer to our Privacy Policy Statement which is posted at our website www.qbe.com/my. If you seek further enquiries, please contact the Personal Data Privacy Officer at telephone number 03-78618400.

I/We do hereby declare that:

1. **I am/we are authorised to make this proposal.**
2. **The answers stated in this proposal are true and complete and I have not withheld any information which may influence the acceptance of this application.**
3. **This application and declaration hereby given shall be the basis of the contract with the Company and I/we will accept the terms, exclusions and conditions which will be set out in the policy to be issued.**
4. **The liability of the Company does not commence until the application has been accepted.**

Proposer's Signature:

Date: (dd/mm/yyyy)

and company stamp

DECLARATION BY AGENT / BROKER / OFFICER (STAFF OF QBE)

In compliance with Section 16(2) of the Anti-Money Laundering Act 2001:

1. **I hereby certify that I have verified and authenticated the Proposer's Business Registration Certificate at the point of sale.**
2. **I have maintained a copy of the Certificate of Incorporation (ROC or ROS) for applicants of group insurance policies where premium is more than RM100,000.00.**

Name

NRIC No

Signature & Company Stamp:

Date: (dd/mm/yyyy)

Clear 8

Summary of cyber coverage

SECTION 1 - CYBER, DATA SECURITY AND MULTIMEDIA COVER

- Liability arising out of multimedia exposures as a result of a hacker. For example defamation, libel and infringement of intellectual property rights
- Liability arising from the failure to properly handle, manage, store, destroy or otherwise control personally identifiable information
- Liability arising out of unintentional transmission of a computer virus
- Liability arising out of a hacker's fraudulent use of information
- The costs of any financial benefit that has been transferred to a third-party that cannot be recouped and has occurred as a result of a covered loss
- The costs to withdraw or alter data or images or other website content as a result of a court order or to mitigate a claim
- The costs to replace or restore documents discovered by the insured to be lost, damaged or destroyed
- Compensation costs arising as a result of directors, partners and employees attending court in connection with a covered claim
- Defence costs

SECTION 2 - DATE BREACH NOTIFICATION COSTS COVER

- The provision of consumer notifications to comply with data breach law following a data breach
- The legal fees incurred to identify notification communication obligations and draft notification communications
- The costs to send and administer notification communications
- The costs of call centre services to respond to enquiries and queries following a notification communication

SECTION 3 - INFORMATION AND COMMUNICATION ASSET RECTIFICATION COSTS COVER

- The costs to repair, restore or replace the affected parts of the insured's information and communication assets after they were damaged, destroyed, altered, corrupted, copied, stolen or misused by a hacker

SECTION 4 - REGULATORY DEFENCE AND PENALTY COSTS COVER

- Payment for those amounts which the insured is legally obliged to pay (including legal and defence costs) as a result of a civil regulatory action, regulatory compensatory award, civil penalty, or fines to the extent insurable by law, imposed by a government or public authority regulator

SECTION 5 - PUBLIC RELATIONS COSTS COVER

- Payment for all reasonable costs the insured incurs for a public relations and crisis management consultant to avert or mitigate any material damage to any of the insured's brands and business operations

SECTION 6 - FORENSICS COSTS COVER

- Payment for a forensic consultant to establish the identity or methods of the hacker or other details required by the insurer following a data breach
- Payment for a security specialist to assess the insured's electronic security and the costs of reasonable security improvement
- Payment for the temporary storage of the insured's electronic data at a third-party host location, if it is viewed that the insureds' information and communication assets remain vulnerable to damage, destruction, alteration, corruption, copying, stealing or misuse by a hacker

SECTION 7 - CREDIT MONITORING COSTS COVER

- Payment for credit monitoring services in order to comply with data breach law

SECTION 8 - CYBER BUSINESS INTERRUPTION COVER

- Payment for loss of business income, as a result of the total or partial interruption, degradation in service, or failure of information and communication assets following a failure by the insured or a service provider to protect against unauthorised access to, unauthorised use of, a denial of service attack against, or transmission of a computer virus to information and communication assets

SECTION 9 - CYBER EXTORTION COVER

- Payment for reasonable and necessary expenses incurred by the insured including the value of any ransom paid by the insured for the purpose of terminating a cyber-extortion threat

ADDITIONAL INFORMATION

Clear 10