Cyber and Data Security Proposal Form

QBE Glqsp_lac&Qgle_nmpc' Nrc Jrb

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
		/ /		
		/ /		
		/ /		
		/ /		

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
%	%	%	%	%	0 %

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	☐	☐	☐		

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	☐	☐	☐
Audits performed	☐	☐	☐
Contract requires security incident to be reported to you	☐	☐	☐

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:

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?

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?

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:

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 authorised 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 QBE of any change in the particulars or statements contained in this proposal form or in the accompanying documents.

Name of business

Signed: Partner, principal or director

Date / /

QBE Insurance (Qgle_nmpc) Nrc Jrb
1 Raffles Quay #29-10
South Tower Singapore 048583
Tel : (65) 6224 6633 • Fax : (65) 6533 3270
www.qbe.com.sg

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

Personal Data Protection Act (PDPA) 2012

Supplementary Consent Clauses

To process, administer and/or manage your relationship, account and policy with QBE Insurance (Singapore) Pte Ltd (QBE), QBE will need to collect, use, disclose and/or process your personal data. Such personal data includes (i) information set out in this [form] and any other personal information provided by you or possessed by QBE; and (ii) your claims.

Such personal data will be collected, used, disclosed and/or processed by QBE for the purpose(s) of:

a) considering whether to provide you with the insurance you applied for;

b) processing your application for underwriting and insurance;

c) administering and/or managing your relationship, account and/or policy with QBE;

d) processing and/or dealing with any claims including the settlement of claims and any necessary investigations relating to the claims, under your policy;

e) carrying out due diligence or other screening activities (including background checks) in accordance with legal or regulatory obligations or risk management procedures that may be required by law or that may have been put in place by QBE;

f) carrying out your instructions or responding to any enquiries by you;

g) dealing in any matters relating to the services and/or products you are entitled to when applying for this or other policies you applied for. This includes the disclosure of some of your personal data when mailing of correspondence, statements, invoices, reports or notices to you, as well as the disclosure of some of your personal data on the cover of envelopes/mail packages;

h) investigating fraud, misconduct, any unlawful action or omission, whether relating to your application, your claims or any other matter relating to your policy, and whether or not there is any suspicion relating to these;

i) compiling a claims history for the purpose of investigation and detecting fraud in present and future claims

j) complying with applicable law in administering and managing your relationship with QBE;

k) providing you with direct marketing communications about QBE's products and services; if you do not want to receive any direct marketing, you may withdraw your consent at any time free of charge by writing in to info.sing@qbe.com

We may/will also be collecting from sources other than yourself, personal data about you, for one or more of the purposes described above, and using, disclosing and/or processing such personal data for one or more of those purposes.

Your personal data may/will be disclosed by QBE to its third party service providers or agents (including its lawyers/law firms), which may be situated outside of Singapore, for one or more of the purposes described above, meaning third party service providers or agents, if engaged by QBE, will be processing your personal data for QBE.

By signing below, you:

- **consent to QBE collecting, using, disclosing and/or processing your personal data for the purposes described above;**
- **consent to QBE collecting personal data about you from sources other than yourself and using, disclosing and/or processing the same, for one or more of the purposes described above;**
- **consent to QBE disclosing your personal data to its third party service providers, or agents (including its lawyers/law firms), for the purposes described above; and**
- **consent to QBE transferring your personal data out of Singapore to its third party service providers, or agents where such third party service providers or agents are sited (whether in Singapore or outside of Singapore), for the purposes described above.**

Name		
B_rc		**Signature**