

Cyber Insurance Proposal Form

Important Notice

The Insurance Act: In this Proposal Form, you are required to disclose fully and faithfully all the facts you know or ought to know in respect of the risk that is being proposed; otherwise the Policy issued hereunder may be void.

Please read the following advice before completing this proposal form.

This proposal is for a claims made policy. A claims made policy only responds to claims made and notified to us during the period of insurance.

The term "PROPOSER" or "You/Your" means the Company (or organisation) listed below and all of its subsidiaries for which coverage is proposed on this form and the "INSURER" or "We/Us/Our" is MSIG Insurance (Singapore) Pte. Ltd.

This PROPOSER is completing this form on behalf of all Insureds (as defined in the policy), it must be signed and dated by an authorised representative of the PROPOSER.

When completing this Proposal Form:

- Answer all questions giving full and complete answers.
- It is your duty to provide all of the information requested on the form as well as to include all material facts.
- A material fact is a known fact and/or circumstance that may influence our decision whether to accept the risk and if so, on what terms. If you are unsure whether a matter is material, you should disclose it. Full details of your duty of disclosure can be found in the following section.
- If the space provided on this form is insufficient, please provide complete answers on an additional sheet, which must be signed and dated.
- The proposal form must be completed, signed and dated by a person, who must be of legal capacity and authorised for the purpose of requesting this insurance by the PROPOSER.

This proposal form DOES NOT BIND the PROPOSER or the INSURER to complete the insurance but will become part of the insurance policy.

YOUR DUTY OF DISCLOSURE

Before you enter into a contract of general insurance with us, you have a duty to disclose every matter within your knowledge that is material to our decision whether to insure you and, if so, upon what terms. You have the same duty to disclose material facts before you renew, extend, vary or reinstate a contract of general insurance.

Your duty however does not require you to tell us anything that:

- Reduces the risk you are insured for; or
- Is common knowledge; or
- We know or, as an insurer, should know; or
- We waive your duty to tell us about.

Note that this duty continues after the proposal form has been completed until the time the policy is in force.

NON-DISCLOSURE

If you fail to comply with this duty of disclosure, we may cancel the policy or reduce the amount we will pay you if you make a claim, or both. If your failure is fraudulent, we may refuse to pay a claim and treat the policy as if it had never existed. It is therefore vital that you make sufficient enquiries before completing this form and before signing the declaration on this form or any addendum; or any declaration that there has been no change in the information you have provided.

SUBROGATION

Where another person or company would be liable to compensate you for any loss or damage otherwise covered by the policy, but you have agreed with that person either before or after the loss or damage occurred that you would not seek to recover any monies from that person or company, we will not cover you under the insurance for such loss or damage.

Section 1 Details of proposer

Company name:

Address of head office:

Web address:

Company registration number:

Place of incorporation:

Date established:

Describe the company's activities:

Section 2 Financial information

1. Please state your turnover:

	Last year (SGD)	Current year (SGD)	Next year estimate (SGD)
Total			
% from online sales			

2. Please show turnover per territory as a percentage of the current year total (All should add up to 100%):

Singapore	Asia	Australia & New Zealand	USA & Canada	Europe	UK	Others

Section 3 Employees

1. Please state you current number of employees per category:

Principals, partners & directors		Information technology	
Professional		Cyber & information security	
Admin & Support		Others (please specify)	

Section 4 Existing data security

1. Is all remote access to your network secured (SSL, SSH, IPSec, etc.)? Yes No

2. Do you have industry grade security measures in place for all firewalls, anti-virus protection and other critical systems? Yes No

If no, please explain what security measures are implemented:

3. Do you have a computer and user account management and audit policy? Yes No

If 'yes', is it enforced? Yes No

If 'no' to either of the above, please explain how account security is maintained:

4. Are all mobile devices and backup media:
 Password protected? Yes No
 Encrypted? Yes No
 If 'no' to either of the above, please explain what security protocols are implemented to secure mobile devices and backup media:

-
5. Are you PCI compliant? Yes No N.A.
6. How often is your important (sensitive, critical, confidential, personal and financial) data backed up? _____
7. Is all your important data encrypted? Yes No
 If 'yes', when does this occur?
 At rest (on network)
 In transit
 In backup
8. Do you ensure that backup data is kept offline/isolated from your enterprise network and that it is inaccessible from all endpoints and servers on your corporate domain?
 If 'yes', is this tested at least annually? Yes No
 Yes No
9. Is your data stored on a flat network? Yes No
10. Are all your employees given mandatory cyber security training?
 If 'yes', how often is this training conducted? Yes No
 Monthly
 Quarterly
 Biannually
 Annually
 Others (please specify) _____
11. Do you distribute written training materials or conduct online refresher training on cyber security for all employees?
 If 'yes', how often? Yes No
 Monthly
 Quarterly
 Biannually
 Annually
 Others (please specify) _____
12. At what intervals are employees required to change passwords?
 Every 90 days or less Yes No
 Less frequently or never (please state) _____
13. Do you have the following policies in place?
 Incident or data breach response plan Yes No
 Disaster recovery or business continuity plan Yes No
 IT security policy or framework Yes No
 If 'yes', please provide copies and state when they were last subject to review: _____
14. Have you ever performed a penetration or social engineering test?
 If 'yes', please provide a copy of the results. Yes No
15. Do you install software patches within 30 days of release? Yes No

16. Have you implemented mandatory multi-factor authentication (MFA) for all remote network access and remote desktop protocol (RDP) connections? Yes No

17. How many employees have administrator rights/admin account access? _____
 How often do you review administrator rights and access? _____
 Is MFA used for administrative account access? Yes No

18. Are you ISO/IEC 27001 Information Security Management compliant? Yes No

19. Do you operate any online platforms or websites? Yes No
 If 'yes', do they use HTTPS? Yes No

20. Do you use an email filter (e.g. Barracuda, Mimecast) on all email accounts? Yes No

Section 5 Outsourced services

1. Do you outsource any of your primary business functions? Yes No
 If 'yes', please state:

Name of provider	Outsourced function

2. Do you outsource any IT functions? Yes No
 If 'yes', please state:

Name of provider	Outsourced function

3. Do you conduct service provider audits to ensure they comply with your security and risk management policies?
 If 'yes', how often are audits conducted?

Monthly
 Quarterly
 Biannually
 Annually
 Others (please specify) _____

4. Have you waived any right of recourse against providers of outsourced services? Yes No

5. What process do you follow to select and manage providers of outsourced services?

6. Are providers of outsourced services required to have their own professional indemnity or errors or omissions cover? Yes No

7. Do you have formal agreements with your outsourced service providers that define each party's responsibilities? Yes No

Section 6 Business interruption

1. Please state your gross profits:

Current year estimate _____

Last financial year _____

2. Does your disaster recovery or business continuity plan address cyber perils? Yes No

3. How critical is your network dependency? Please state the time interval between loss of site or systems and significant impact on your business operations:

0 to 6 hours

6 to 12 hours

12 to 24 hours

A day or more

Section 7 Personal data

1. How many personal data and Personally Identifiable Information (PII) records do you store? _____

2. Please show records per territory as a percentage:

Singapore	Asia	Australia & New Zealand	USA & Canada	Europe	UK	Others

3. State the number of records held in each of the following categories:

Personal (name, email, residential address, telephone or mobile number)	
Date of birth	
Bank details including account data, debit and credit cards	
Health information	
Tax records, including tax file numbers and references	
Others, please describe	

4. Do you handle credit card transactions in any form? Yes No

If 'yes', how many per year? _____

5. Do you use a secure payment processor for credit card transactions? Yes No

Please provide details:

6. What percentage of personal data records are held on:

Your own network _____

Last financial year _____

7. Please provide an estimate of the maximum number of personal records currently stored: _____

On any single server _____

In any central/single location _____

Section 8 Regulatory

1. Have you ever been subject to an investigation into your handling of PII or personal data, payment card details or your data privacy practices? Yes No
2. Has a regulator or similar authority ever requested information on your handling of PII or personal data, payment card details or your data privacy practices? Yes No
3. Have you ever been asked to sign (or signed) a consent order or equivalent in respect of PII or your privacy practices? Yes No
4. Have you ever received a complaint relating to your handling of PII? Yes No

If you have answered 'yes' to any question, please provide details:

Section 9 Claim history

Please ensure appropriate enquiries are made of all directors and officers of the company prior to answering the following questions.

1. Have you ever suffered a loss or has any claim been made against you, whether successful or not? Yes No
2. Are you aware of any circumstance, incident or action which may be grounds for or result in a future claim? Yes No

If you have answered 'yes' to any question, please provide details:

Section 10 Previous insurance cover

1. Do you currently have cyber liability and data protection insurance? Yes No
If 'yes', please state:

Insurer	
Limit of liability	
Expiry date	
Retroactive date (if applicable)	
Deductible	

2. Has your company or any subsidiary ever been refused this type of insurance, or had similar insurance cancelled, or had an application of renewal declined, or had special terms imposed? Yes No
If 'yes', please supply details:

Section 11 Indemnity limit

Limit of indemnity required:

- SGD500,000
 SGD1,000,000
 SGD2,000,000
 Other SGD _____

Section 12 Declaration

I/We, the undersigned, desire to effect the insurance specified herein and declare that I/We:

- have read and understood the Important Notice.
- agree that MSIG Insurance (Singapore) Pte. Ltd. reserves its right to reject this application and cover will only be effective when accepted and confirmed in writing.
- warrant that the information and any documents given and answers to questions herein are true and correct to the best of my/our knowledge.
- have not withheld, misstated or omitted facts likely to influence the assessment of this application.
- undertake to inform MSIG Insurance (Singapore) Pte. Ltd. of any material changes to those facts before completion of the contract of insurance.
- agree that this application, declaration and any other information provided or documents supplied shall form the basis of the contract of insurance.
- agree and acknowledge that the contract of insurance will be subject to the terms, limitations, exclusions, conditions, clauses and warranties contained in the policy and/or as modified or extended by any endorsements thereon.

Privacy Policy

MSIG is committed to protecting your privacy. We collect, use and disclose the personal particulars you provide to us in accordance with the Personal Data Protection Act 2012 and MSIG's Privacy Policy, for the provision of all services related to, and protection under the insurance policy purchased from us, including for proper servicing, underwriting and claims administration. MSIG may disclose the personal particulars to its business partners and third party service providers for these purposes. Where there are more than one individual insured persons, I/we confirm they have consented to MSIG's collection, use and disclosure of their personal particulars. Please refer to the full MSIG's Privacy & Cookies Policy at www.msg.com.sg for more information.

Authorised signature (with company stamp)

Date

Name & position