

## Cyber Insurance Proposal Form

### Important Notice

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 (Hong Kong) Limited.

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:	Company registration number:
Address of head office:	
Web address:	
Place of incorporation:	Date established:
Describe the company's activities:	

## Section 2 Financial information

1. Please state your turnover:

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

2. Please show turnover per territory as a percentage of the current year total:

Hong Kong & Macau	Asia	Australia & New Zealand	USA & Canada	Europe	UK	Others
%	%	%	%	%	%	%

## Section 3 Employees

1. Please state your 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. How often is your important (sensitive, critical, confidential, personal and financial) data backed up? _____			
7. Is all your important data encrypted? If 'yes', when does this occur?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<input type="checkbox"/> At rest (on network)			
<input type="checkbox"/> In transit			
<input type="checkbox"/> 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
9. Is your data stored on a flat network?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
10. Are all your employees given mandatory cyber security training? If 'yes', how often is this training conducted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<input type="checkbox"/> Monthly			
<input type="checkbox"/> Quarterly			
<input type="checkbox"/> Biannually			
<input type="checkbox"/> Annually			
<input type="checkbox"/> 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<input type="checkbox"/> Monthly			
<input type="checkbox"/> Quarterly			
<input type="checkbox"/> Biannually			
<input type="checkbox"/> Annually			
<input type="checkbox"/> Others (please specify) _____			
12. At what intervals are employees required to change passwords? Every 90 days or less Less frequently or never (please state) _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
13. Do you have the following policies in place? Incident or data breach response plan Disaster recovery or business continuity plan IT security policy or framework If 'yes', please provide copies and state when they were last subject to review: _____	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
14. Have you ever performed a penetration or social engineering test? If 'yes', please provide a copy of the results.	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
15. Do you install software patches within 30 days of release?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
16. Have you implemented mandatory multi-factor authentication (MFA) for all remote network access and remote desktop protocol (RDP) connections?	<input type="checkbox"/> Yes	<input type="checkbox"/> 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
18. Are you ISO/IEC 27001 Information Security Management compliant?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
19. Do you operate any online platforms or websites? If 'yes', do they use HTTPS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
20. Do you use an email filter (e.g. Barracuda, Mimecast) on all email accounts?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

## Section 5 Outsourced services

1. Do you outsource any of your primary business functions?  
If 'yes', please state:

Yes  No

Name of provider	Outsourced function

2. Do you outsource any IT functions?  
If 'yes', please state:

Yes  No

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 MOP \_\_\_\_\_

Last financial year MOP \_\_\_\_\_

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:

Hong Kong & Macau	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 \_\_\_\_\_ %

3<sup>rd</sup> party networks \_\_\_\_\_ %

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

1. Limit of indemnity required:

- |  |  |
|--|--|
| <input type="checkbox"/> MOP 5,000,000   | <input type="checkbox"/> USD 1,000,000   |
| <input type="checkbox"/> MOP 10,000,000  | <input type="checkbox"/> USD 2,000,000   |
| <input type="checkbox"/> MOP 30,000,000  | <input type="checkbox"/> USD 5,000,000   |
| <input type="checkbox"/> Other MOP _____ | <input type="checkbox"/> Other USD _____ |

## Section 12 Declaration

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

- agree that MSIG Insurance (Hong Kong) Limited reserves its right to reject my application.
- warrant that the information given and answers to questions herein are true and correct to the best of my/our knowledge.
- have not withheld facts likely to influence assessment of this application.
- agree that this application, declaration and other information provided shall form the basis of the contract and agree to accept the terms, limitations, exclusions, conditions, clauses and warranties contained in the policy/policies and/or as modified or extended by any endorsements thereon.

### Declaration of Broker Commission (if applicable)

The applicant understands, acknowledges and agrees that, as a result of the applicant purchasing and taking up the policy to be issued by MSIG Insurance (Hong Kong) Limited ("MSIG"), MSIG will pay the authorised insurance broker commission during the continuance of the policy including renewals, for arranging the said policy. Where the applicant is a body corporate, the authorised person who signs on behalf of the applicant further confirms to MSIG that he or she is authorised to do so. The applicant further understands that the above agreement is necessary for MSIG to proceed with the application.

## Appendix: Notice to customers relating to Law no. 8/2005 Personal Data Protection Act ("the Act")

MSIG Insurance (Hong Kong) Limited ("MSIG", "we" or "us") would ask that you take the time to read this privacy policy carefully. In case of discrepancies between the English and Chinese versions of this statement, the English version shall prevail.

### Privacy Policy

MSIG takes your privacy very seriously. To ensure your personal information is secure, we communicate and enforce our privacy and security guidelines according to the relevant laws and regulations. MSIG takes precautions to safeguard your personal information against loss, theft, and misuse, as well as against unauthorised access, disclosure, alteration, and destruction. Furthermore, we will not sell your personal information to anyone without your consent. MSIG imposes very strict sanction control and only authorised staff on a need-to-know basis are given access to or will handle your personal data, and we provide regular training to our staff to keep them abreast of any new developments in privacy laws and regulations.

We will only retain your personal data in our business records for as long as it is necessary for business and tax purposes as permitted by the laws. We will require our agents, contractors or third parties who provides administrative or other services on our behalf to protect personal data they may receive in a manner consistent with this policy. We do not allow them to use such information for any other purposes. If you have any questions or inquiries regarding our Privacy Policy, please feel free to contact us.

We may amend this Privacy Policy at any time and for any reason. The updated version will be available by following the 'Privacy Policy' link on our website homepage at [msig.com.hk](http://msig.com.hk). You should check the Privacy Policy regularly for changes.

### Personal Information Collection Statement

Personal information is data that can be used to uniquely identify or contact a single person. As our customer, it is necessary from time to time for you to supply us with your personal data in relation to the general insurance services and products ("the Product") that we provide to you and in order for us to deliver and improve customer service. This includes but not limited to the personal data contained in the proposal form or in any documents in relation to the Product or any claim made under the Product.

If you do not provide us with your personal data, we may not be able to provide the Product you need or process your request.

We may use your personal data for:-

- processing and evaluating your insurance application and any variation or renewal of the Product;
- administration of the services and facilities in relation to the Product provided to you;
- conducting identity and/or credit checks;
- invoicing, processing payment instructions and collecting premiums and outstanding amounts from you;
- assessing and processing claims in relation to the Product;
- conducting statistical or actuarial research and/or analysis by us;
- automated decision-making processes, including profiling, for risk assessment and claims management;
- other ancillary purposes which are directly related to the above purposes;
- conducting matching procedures or similar activities as defined under the relevant laws in Macau;
- complying with applicable laws, regulations or any industry codes or guidelines; and
- detecting, investigating and preventing fraud and/or other illegal activity (whether or not relating to the Product issued in respect of this application).

In connection with any of the above purposes, the personal data that we have collected might be disclosed or transferred to the following persons and/or entities (who may be located within or outside of Macau, or may process or store your personal data outside of Macau):

- third party agents, contractors, service providers and advisors (including but not limited to debt collection agencies, credit reference bureaus or call centers) who provide administrative, communications, computer, data processing and storage, payment, security, information technology, marketing or other services which assist us to carry out the above purposes (including medical service providers, emergency assistance

- service providers, telemarketers, mailing houses, IT service providers and data processors);
- loss adjudicators, claims investigators and medical advisors;
- reinsurers and reinsurance brokers;
- your insurance intermediary;
- our legal and professional advisors;
- our related companies that are part of our corporate group, including, without limitation, any parent company, subsidiary, affiliate, or any other entity under common ownership or control, as defined under the related laws in Macau;
- Macau Insurers' Association (or any similar insurance industry association or federation);
- government agencies and authorities as required or permitted by law;
- the police and fraud investigation or prevention organizations;
- databases or registers (and their operators) used by the insurance industry to analyse and check information provided against existing information; and
- in the event that we transfer all or a substantial part of our business to another company, the transferee of that business, who may then use your personal data to continue carrying out that business.

In order to confirm the accuracy of your personal data, you agree to provide us with authorisation to access and to verify any of your personal data with the information collected by any federation of insurance companies from the insurance industry.

MSIG also intends to use your name, your address, your phone number and email address from time to time to provide marketing materials and conduct direct marketing (including but not limited to promotion, marketing and sales) of the Product.

**If you do not wish MSIG to use your personal data for direct marketing as listed above, you should tick the box on the right and send us a copy of this Notice at the address listed below together with the required information which are necessary for us to process your opt-out request. You may also notify us by filling in the "Enquiry form – Opt-out from direct marketing activities" on our website at [msig.com.hk](http://msig.com.hk). In your notification, you must supply the same required information as listed below.**



**To enable us to process your opt-out request, please provide us below information and send to: The Data Protection Officer at Avenida Da Praia Grande No. 693, Edif Tai Wah 13 Andar A&B, Macau.**

**Full name:**

**Contact number:**

**Macau ID number:** *(for identification purpose)*

**Policy/Certificate/Acknowledgement number**  
*(if you have one):*

**Note: This instruction will override all previous instructions relating to direct marketing that have been given to MSIG.**

Under the Act, you have the right to: (a) be informed of the kind of personal data held by us; (b) be informed of the main purposes for which personal data held by us are or are to be used; (c) request access to your personal data held by us; (d) request correction of your personal data held by us; and (e) ascertain our policies and practices in relation to personal data. If you wish to exercise these rights, please write to our Data Protection Officer at Avenida Da Praia Grande No. 693, Edif Tai Wah 13 Andar A&B, Macau.

If you have any enquiries or require assistance with this Personal Information Collection Statement, please call us at +853 2892 3329.

Authorised Signature (with Company Chop)

\_\_\_\_\_  
Name and position

Date \_\_\_\_\_ (DD/MM/YYYY)