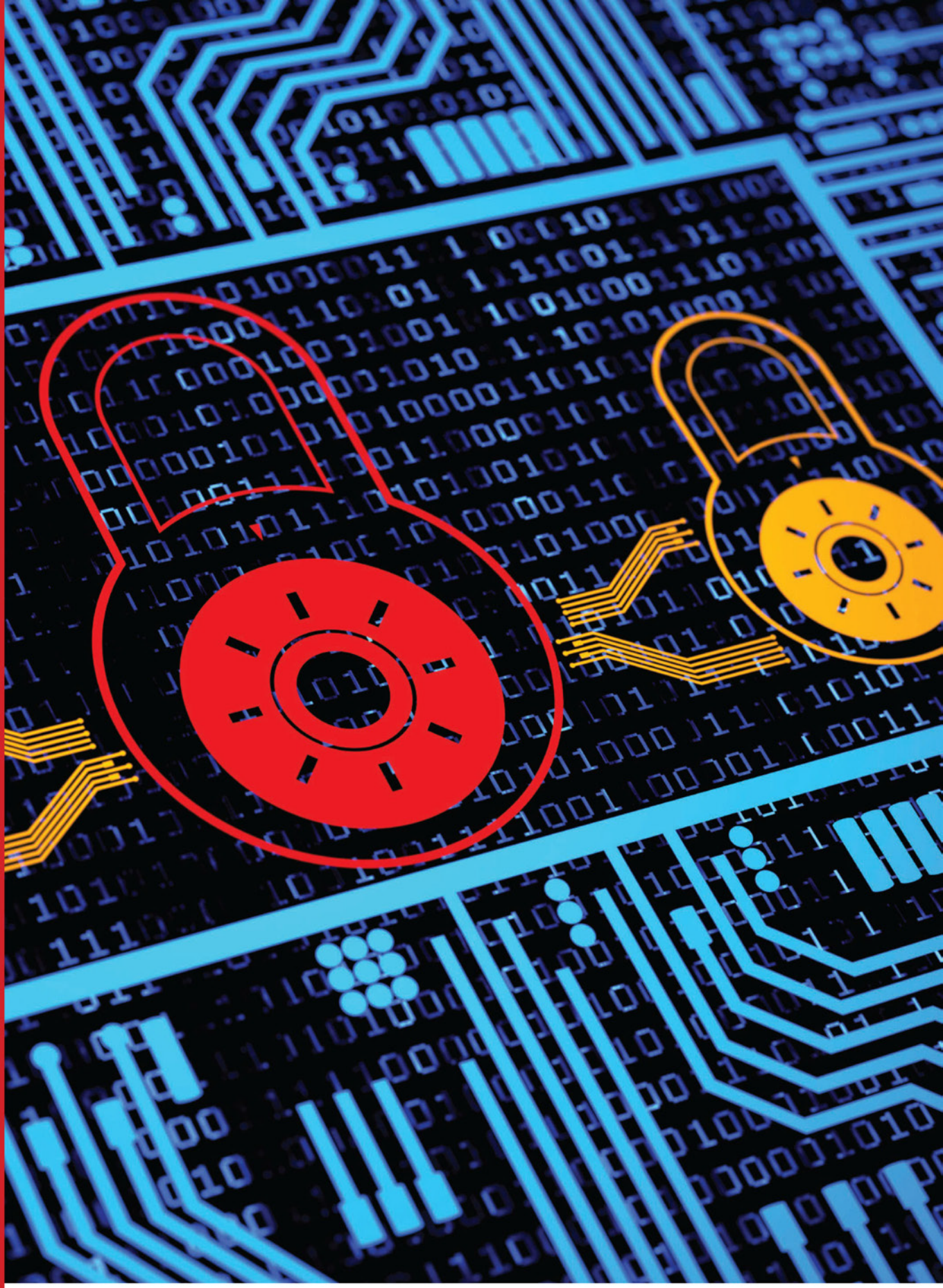
Cyber Proposal Form



Suite 201, 272 Pacific Highway,
Crows Nest NSW 2065, Australia

t 02 8912 6400

www.lauw.com.au

LAUW
LONDON AUSTRALIA UNDERWRITING

IMPORTANT NOTICES

Pursuant to the provisions of the Insurance Contracts Act 1984 (Cth), Underwriters are required to notify you of the following relevant information.

Your Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms.

You have this duty until we agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell us anything that:

- reduces the risk we insure you for; or
- is common knowledge; or
- we know or should know as an insurer; or
- we waive your duty to tell us about.

If you do not tell us something

If you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both.

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

It should be noted that this duty continues until the Policy is entered into with Underwriters, and extends to any renewal, reinstatement, variation or extension to the Policy.

Non-Disclosure

Underwriters may be entitled to either reduce their liability under the contract in respect of a Claim, cancel the contract or avoid the contract from its beginning in accordance with the provisions of the Insurance Contract Act 1984 (Cth) if you fail to comply with your duty of disclosure.

Claims Made

This is a "claims made" policy of insurance, which means that it only covers claims made against an insured and notified to Underwriters during the period of insurance. By operation of Section 40(3) of the Insurance Contracts Act 1984 (Cth), where the insured gives notice in writing to the insurer of facts that might give rise to a claim against the insured as soon as was reasonably practicable after the insured became aware of those facts but before the insurance cover provided by the contract expired, the insurer is not relieved of liability under the contract in respect of the claim, when made, by reason only that it was made after the expiration of the period of the insurance cover provided by the contract.

Retroactive Liability

The policy may be limited by a retroactive date stated in the schedule. The policy does not provide cover in relation to any claim arising from any actual or alleged act, error, omission or conduct that occurs before the commencement of the policy, unless retroactive liability cover is extended by Underwriters.

Liability Assumed Under Agreement

Cover provided by this form of liability insurance does not cover liability which you have agreed to accept unless you would have been so liable in the absence of such agreement.

Utmost Good Faith

In accordance with Section 13 of the Insurance Contracts Act 1984 (Cth), the policy of insurance is based on utmost good faith requiring Underwriter(s) and the proposer / insured(s) to act towards each other with the utmost good faith in respect of any matter relating to the insurance contract.

Privacy Notice

LAUW and **Underwriters** are committed to compliance with the provisions of the Australian Privacy Principles and the Privacy Act 1988 (Commonwealth). In order for **Underwriters** to assess the risk of and provide you with insurance products and assess and manage any claims under those products, it is necessary to obtain personal information from you. If you do not provide us with this information, this may prevent **Underwriters** from providing you with the products or services sought.

If you provide us with information about someone else, you must obtain their consent to do so. LAUW and **Underwriters** may disclose your information to other insurers, their reinsurers, and insurance reference service or other advisers used by **Underwriters** or LAUW on behalf of **Underwriters** such as loss adjusters, lawyers or others who may be engaged to assist in claims handling, underwriting or for the purpose of fulfilling compliance and/or regulatory requirements. These third parties will all be contractually required to adhere to **Underwriters**' privacy obligations.

Our privacy policy contains information about how you can access the information we hold about you, ask us to correct and how you may make a privacy related complaint. You can obtain a copy of our privacy policy here.

Should you require access to your personal information, LAUW may be contacted on (02) 8912 6400.

LAUW
London Australia Underwriting

Cyber eRisks Insurance Proposal Form

Important: Please answer all questions fully. All questions will be deemed to be answered in respect of all entities & persons to be insured under this policy. If the space provided is insufficient please include attachments on your company letterhead

Section 1: General Information

a.) Name of Insured(s) (Include all entities to be Insured including Subsidiaries)

b.) Address of the principal office (please provide a street address only.)

Street

City

State

Country

Postcode

c.) Contact details

Name

Telephone

Email

Website

d.) When was your business established?

e.) Please provide a brief overview of business operations of proposed/insured entities

f.) Please provide revenue details as per below.

Location	Last Completed Financial Year	Current Financial Year Forecast	Next Financial Year
Australia & New Zealand			
USA & Canada			
Other			
Total			

g.) Please provide a breakdown of your revenue generated in the last financial year as follows:

ACT	%	NSW	%	NT	%	QLD	%	Overseas
SA	%	TAS	%	VIC	%	WA	%	%

h.) Number of employees

Section 2: Business Information

a.) Do you allow online purchases, bill payment, banking or trading?

☐ **Yes** ☐ **No**

If 'Yes" what proportion of revenue is received through the online distribution channel?

b.) What type of personal information do you collect, process and store? (Please tick those relevant)

☐ Business and Customer Information ☐ Health Care information ☐ Financial Account Information

☐ Credit Card Information ☐ Tax File Number ☐ Social Security Number

☐ Intellectual Property/Trade Secrets ☐ Other 'Please Specify'

c.) Approximately how many Individual's records have you collected or stored on your network?

d.) Do you share any personal/sensitive information with business partners, vendors or other third parties?

☐ **Yes** ☐ **No**

e.) Do you transfer personal/sensitive information across international borders?

☐ **Yes** ☐ **No**

f). Do you outsource any primary business functions to a third party?

☐ **Yes** ☐ **No**

If 'Yes' please describe (for example information technology, human resources etc)

g.) Do you have agreements in place with your service providers that confirm a level of security which is equal to or better than your own security?

☐ **Yes** ☐ **No**

h) Do you require third parties with which you share personally identifiable information or confidential information, to indemnify you for legal liability arising out of the release of such information due to the fault or negligence of the third party?

☐ **Yes** ☐ **No** ☐ **N/A**

Section 3: Organisational Governance

a.) Do you have a senior executive responsible for records and information management?

☐ **Yes** ☐ **No**

If 'Yes', please indicate the job title of this executive i.e. Chief ISO and if 'No' who is responsible?

b.) Do you publish and distribute written computer and information security procedures to employees?

☐ **Yes** ☐ **No**

c.) Are security risk assessments conducted on at least an annual basis to ensure security policies are being followed?

☐ **Yes** ☐ **No**

d.) Are privacy risk assessments conducted on at least an annual basis to ensure privacy policies are being followed?

☐ **Yes** ☐ **No**

e.) Are these results shared with the executive management team and are key issues remediated and resolved?

☐ **Yes** ☐ **No**

f.) Do you have any of the following (Please provide copies of these documents):

i) Disaster recovery plan? ☐ **Yes** ☐ **No**

ii) Business continuity plan? ☐ **Yes** ☐ **No**

iii) Incident response plan for network intrusions and virus incidents? ☐ **Yes** ☐ **No**

Are such plans tested annually and if not how often are they tested?

g.) Do the results of these tests confirm you can be back up and running within 24 hours or sooner?

☐ **Yes** ☐ **No**

h.) Is all valuable/sensitive data backed-up on a daily basis?

☐ **Yes** ☐ **No**

If 'Yes', where to?

If 'No', please describe exceptions.

i.) How often are virus signatures updated? (Please tick)

☐ Automatic ☐ Weekly ☐ Monthly ☐ Other:

j.) Do you enforce software update processes with the installation of software patches?

☐ **Yes** ☐ **No**

k.) Are critical patches installed within 30 days of release?

☐ **Yes** ☐ **No**

l.) Please describe your network infrastructure vendors.

Network security

Cloud/back-up

ISP

Business critical software provide

Payment Processor

POS hardware provider

m.) Are you subject to Payment Card Industry (PCI) Security Standards?

☐ **Yes** ☐ **No**

If 'Yes' please indicant your merchant level

☐ 1 ☐ 2 ☐ 3 ☐ 4

n.) If yes to Question m) have you achieved PCI compliance?

☐ **Yes** ☐ **No**

Section 4: Network Security

a.) Are systems, applications and supporting infrastructure that collect, process or store personal information segregated from the rest of the network?

☐ **Yes** ☐ **No**

b.) Is firewall technology used at all internet points of presence and do formal firewall configuration standards exist?

☐ **Yes** ☐ **No**

c.) Are firewalls installed between all wireless networks and system components that process or store personal information?

☐ **Yes** ☐ **No**

d.) Are internal and external vulnerability scans and penetration tests (network and application layer) conducted on a periodic basis and the vulnerabilities identified, tracked and remediated?

☐ **Yes** ☐ **No**

e.) Do all users of systems, applications and supporting infrastructure that collect, process or store personal information have a unique ID?

☐ **Yes** ☐ **No**

f.) Is 2-factor authentication utilized for all remote access (e.g. VPN) to the internal network?

☐ **Yes** ☐ **No**

g.) Do password policies and procedures exist that outline strong password requirements (e.g. change of passwords on a periodic basis, use of numeric and alphabetic characters, prohibition of previously used passwords)?

☐ **Yes** ☐ **No**

h.) Is user access to systems, applications and supporting infrastructure that collect, process or store personal information removed in a timely manner upon employee termination, job change or cancellation of a third party vendor agreement?

☐ **Yes** ☐ **No**

i.) Do removable media handling procedures exist for the internal or external distribution of media that contain personal information?

☐ **Yes** ☐ **No**

Section 5: Data Management

a.) Do procedures exist to monitor for new vulnerabilities within system components and apply the latest security patches within one month?

☐ **Yes** ☐ **No**

b.) Do you utilise anti-virus software on all systems commonly affected by viruses, particularly personal computers and servers?

☐ **Yes** ☐ **No**

c.) Does your anti-virus programs detect, remove, and protect against other forms of malicious software, including spyware and adware?

☐ **Yes** ☐ **No**

e.) Do procedures exist to operationalise the proper disposal of personal information and data and have they been implemented in compliance with your organisation's confidential data disposal policy?

☐ **Yes** ☐ **No**

f.) Do you have and enforce policies concerning when internal and external communication should be encrypted?

☐ **Yes** ☐ **No**

g.) Do you encrypt all sensitive and confidential data stored on laptop computers and portable media?

☐ **Yes** ☐ **No**

h.) Do you encrypt all sensitive and confidential data stored on back-up tapes?

☐ **Yes** ☐ **No**

i.) Do you encrypt all sensitive and confidential data when at rest on the network?

☐ **Yes** ☐ **No**

j.) Do you encrypt all sensitive and confidential data when in transit from the network?

☐ **Yes** ☐ **No**

Section 6: Multimedia

a.) Do you publish any blogs, newsletters, videos, podcasts or other similar publications?

☐ **Yes** ☐ **No**

If 'Yes', what processes and controls are in place for editing and/or reviewing such communications prior to publication?

b.) Are legal reviews always sought prior to the publication of new content?

☐ **Yes** ☐ **No**

c.) Do you use public materials which include intellectual property owned by third parties?

☐ **Yes** ☐ **No**

If 'Yes', is consent in writing or a license always obtained from the owner of such material?

☐ **Yes** ☐ **No**

d.) Does your website allow third parties to publish content on chat rooms, comment boxes or any other publically viewable space?

☐ **Yes** ☐ **No**

If 'Yes' is such content moderated prior to its publication?

☐ **Yes** ☐ **No**

Section 7: Claims/Incident History & Prior Insurance

a.) Do you have any insurance currently in place that covers any element of risk also covered by a cyber policy (cyber may be found in extended property, crime, D&O/ML or E&O/PI policies)?

☐ **Yes** ☐ **No**

If "yes' please provide details

b.) In the past 5 years have your ever been declined or had your cyber insurance cancelled?

☐ **Yes** ☐ **No** *** If 'yes' please attach a detailed description of the circumstance(s)**

c.) In the past 5 years have you sustained significant systems intrusion, data theft or other loss of data?

☐ **Yes** ☐ **No** *** If 'yes' please attach a detailed description of the circumstance(s)**

d.) In the past 5 years have you been notified by any third party that personally identifiable information has been compromised from your systems?

☐ **Yes** ☐ **No** *** If 'yes' please attach a detailed description of the circumstance(s)**

e.) In the past 5 years, have you notified customers that their Personally Identifiable information was compromised from your systems?

☐ **Yes** ☐ **No** *** If 'yes' please attach a detailed description of the circumstance(s)**

f.) Have you ever been the subject of an investigation by a regulatory or other government agency arising out of a privacy issue?

☐ **Yes** ☐ **No** *** If 'yes' please attach a detailed description of the circumstance(s)**

g.) Are you or any of your former or current directors, officers, employees, subsidiaries or independent contractors aware of any claims or circumstances of any nature that may be covered under this policy?

☐ **Yes** ☐ **No** *** If 'yes' please attach a detailed description of the circumstance(s)**

Declaration:

I/We hereby declare that:

My/Our attention has been drawn to the Important Notice on page 2 of this Proposal form and further I/we have read these notices carefully and acknowledge my/our understanding of their content by my/our signature/s below.

The above statements are true, and I/we have not suppressed or mis-stated any facts and should any information given by me/us alter between the date of this Proposal form and the inception date of the insurance to which this Proposal relates I/we shall give immediately notice thereof.

I/We authorise insurers to collect or disclose any personal information relating to this insurance to/from any other insurers or insurance reference service. Where I/we have provided information about another individual (for example, an employee, or client).

I/We also confirm that the undersigned is/are authorised to act for and on behalf of all persons and/or entities who may be entitled to indemnity under any policy which may be issued pursuant to this Proposal form and I/we complete this Proposal form on their behalf.

To be signed by the Chairman/President/Managing Partner/Managing Director/Principal of the association/partnership/company/practice/business.

Signature	Date	Signature	Date
SIGN		SIGN	

It is important the signatory/signatories to the Declaration is/are fully aware of the scope of this insurance so that all questions can be answered.

If in doubt, please contact your insurance broker since non-disclosure may affect an Insured's right of recovery under the policy or lead to it being avoided.

OPTIONAL COVER(S)

Reputational Harm (Contingent Business Interruption)

☐ Yes ☐ No

Limits: $250,000 ☐ $500,000 ☐ $1,000,000 ☐

Tangible Property (Bricking) - $25,000

☐ Yes ☐ No

Cyber Crime

☐ Yes ☐ No

If "yes" to Cyber Crime, please complete the following questions.

1. Limits: $25,000 ☐ $50,000 ☐ $75,000 ☐ $100,000 ☐ $150,000 ☐

2. Can the Proposer confirm that the following operations are always segregated so that no individual person can control any operation from start to finish without referral to another person?

   a) Cheques being signed or payments being authorised above AUD$10,000 ☐ Yes ☐ No

   b) Issuing funds transfer instructions ☐ Yes ☐ No

   c) Amending funds transfer procedures ☐ Yes ☐ No

   d) Opening new bank or supplier accounts ☐ Yes ☐ No

   e) Refund of monies or return of goods above AUD$10,000 ☐ Yes ☐ No

3. Can the Proposer confirm that bank statements are always independently reconciled by persons who are not authorised to deposit and/or withdraw funds or issue funds transfer instructions? ☐ Yes ☐ No

4. Can the Proposer confirm whether an independent physical count of stock, raw materials, work in progress and finished goods is undertaken and whether the count is then reconciled against recorded stock levels? ☐ N/A ☐ Yes ☐ No

   a) How frequently is a count undertaken?

   b) Were there any discrepancies discovered during the most recent count? ☐ Yes ☐ No

   If "Yes" to question 4b), please provide full details or attach an addendum:

5. Does the Firm have an approved suppliers list that is regularly updated and checked by the Directors or Officers? ☐ Yes ☐ No

6. Can the Proposer confirm that all suppliers, service providers and outsourcing companies are

   a) vetted for competency, financial stability and honesty before being approved? ☐ Yes ☐ No

   b) appointed under a written contract? ☐ Yes ☐ No

   If "No" to any part of question 7, please provide full details:

7. Does the proposer accept funds transfer instructions over the telephone, fax, email or some other electronic communications method?

   ☐ Yes ☐ No

8. Do employees receive anti-fraud training including but not limited to detection of impersonation fraud or phishing scams?

   ☐ Yes ☐ No ☐ N/A

9. Does the proposer verify any request to transfer funds made by an employee, officer or owners by calling back the employee, officer or owner at the telephone number listed in the company directory?

   ☐ Yes ☐ No ☐ N/A

10. Does the proposer have procedures in place to verify the authenticity of any payment or funds transfer request received by an employee from an internal company source (e.g. another employee, subsidiary, location or department)?

    ☐ Yes ☐ No ☐ N/A

11. Within the last three years, has the Firm discovered any employee dishonesty, burglary, robbery, disappearances, destruction or forgery losses?

    ☐ Yes ☐ No

    If "Yes," please provide full details or attach an addendum:

12. Has the Firm ever been declined, had cancelled or non-renewed any insurance policy for Cyber Crime coverage?

    ☐ Yes ☐ No

    If "Yes," please provide full details or attach an addendum:

I/We declare that the above answers, statements, particulars and additional information are true to the very best of the knowledge and belief of the Proposer. After full enquiry, I/We also confirm that I/We have disclosed all information and material facts that may alter the Underwriters' view of the risk,or affect their assessment of the exposures they are covering under the policy. I/We understand that all answers, statements, particulars and additional information supplied with this proposal form will become part of and form the basis of the policy.

I/We acknowledge that we have read and understood the content of the Important Notice contained in this proposal.

Signed:

Name in capital letters (printed):

Date:

Position:

For and/on behalf of the **Proposer**: