AUSTBROKERS CYBER PRO

Cyber Insurance Proposal Form (Corporate)

Important Notice

Claims Made Insurance

This is a proposal for a 'Claims Made' policy of insurance. This means that the policy covers you for any claims made against you and notified to the insurer during the policy period. The policy does not provide cover in relation to:

- acts, errors or omissions that occurred prior to the retroactive date (if one is specified) in the policy;
- any claim made, threatened or intimated against you prior to the commencement of the policy period;
- any claim or fact that might give rise to a claim, reported or which can be reported to an insurer under any insurance policy entered into before the commencement of the policy period;
- any claim or fact that might give rise to a claim, noted in this proposal or any previous proposal;
- any claim arising out of any fact you are aware of before the commencement of the policy period;
- any claim made against you after the expiry of the policy period.

However, the effect of Section 40(3) of the Insurance Contracts Act 1984 (Cth) is that where you become aware, and notify us in writing as soon as is reasonably practicable after first becoming aware but within the policy period, of any facts which might give rise to a claim against you, any claim which does arise out of such facts shall be deemed to have been made during the policy period, notwithstanding that the claim was made against you after the expiry of the policy period.

Your Duty of Disclosure

Before you enter into a contract of general insurance with an insurer, you have a duty, under the Insurance Contracts Act 1984 (Cth), to disclose to the insurer every matter that you know, or could reasonably be expected to know, is relevant to the insurer's decision whether to accept the risk of the insurance and, if so, on what terms.

You have the same duty to disclose those matters to the insurer before you renew, extend, vary or reinstate a contract of general insurance.

Your duty however does not require disclosure of matter:

- that diminishes the risk to be undertaken by the insurer;
- that is of common knowledge;
- that your insurer knows or, in the ordinary course of its business, ought to know;
- as to which compliance with your duty is waived by the insurer.

Non Disclosure

If you fail to comply with your duty of disclosure, the insurer may be entitled to reduce their liability under the contract in respect of a claim or may cancel the contract. If your non-disclosure is fraudulent, the insurer may also have the option of avoiding the contract from its beginning.

Privacy Policy

We are bound by the Privacy Act 1988 (Cth) and the Privacy Amendment (Enhancing Protection) Act 2012 (Cth) or as amended, and its associated National Privacy Principles when we collect and handle your personal information. We collect personal information in order to provide our services. We also pass it to third parties involved in this process such as insurers and other service providers. If you do not provide the information we need we may not be able to offer you insurance or deal with claims under your insurance.

When you give us personal or sensitive information about other individuals, we rely on you to have made or make them aware that you will or may provide their information to us, the purposes we use it for, the types of third parties that we disclose it to and how they can access it. If it is sensitive information we rely on you to have obtained their consent on these matters. If you have not done either of these things, you must tell us before you provide the relevant information.

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 income generated in the last financial year as follows:

ACT % NSW % NT % QLD %

SA % TAS % VIC % WA % Overseas %

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?

- ☐ 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? (Multiple pieces of information on the same individual can be considered as one record)

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.) If yes to Question f.) do you allow a third party to host your data and if so please provide the name of the third party and their location. Yes ☐ No ☐

h.) If yes to Question g.) do you ensure your service providers have adequate security measures in place? Yes ☐ No ☐

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.) Describe how employees and contractors with access to your company's network are trained in matters such as cyber security, privacy awareness and compliance.

c.) Do you have a company-wide policy that addresses compliance with privacy and data protection laws or regulations as required for your business, industry or required by jurisdictions where you conduct business and is it reviewed by an independent 3rd party? Yes ☐ No ☐

If 'no', please describe how you address privacy and data protection laws within your organisation?

d.) Do you or your cloud hosting provider, back-up your critical data at least once per week and store these back-ups in a location that is separate from your physical premises e.g. segregated from your network?

Yes ☐ No ☐

e.) Do you have a documented Incident Response or Business Continuity Plan in place which covers network security incidents and is tested at least annually? Yes ☐ No ☐

If 'no', please describe how business continuity is maintained and the recovery time objectives met.

f.) Please provide details of the data backed up (Please tick all that apply):

☐ Critical data only
☐ Infrastructure (Operating system and device configuration)
☐ Applications
☐ All data
☐ Other

g.) How often are back-ups tested for recovery integrity?

☐ Quarterly, or more regularly
☐ Bi-annually
☐ Annually
☐ Other

h.) Please describe your network infrastructure vendors.

- Firewall
- Anti-virus
- ISP
- Intrusion Detection

Section 4: Network Security & Data Management

a.) Are systems, applications and supporting infrastructure that collect, process or store personal information segregated from the rest of the network? Yes ☐ No ☐

b.) Do you have firewall technology at all internet points of presence and do formal (e.g. not default) firewall configurations exist? Yes ☐ No ☐

c.) Do you, or your IT outsourced service provider, have a patch management policy in place that enables you to implement critical patches within 30 days? Yes ☐ No ☐

d.) Do you have anti-malware software installed and enabled on all desktops, laptops and servers (excluding database servers) and is it updated automatically? Yes ☐ No ☐

e.) Have you implemented advanced endpoint protection for malware detection?

Yes ☐ No ☐

If 'yes' to (e), which solution provider?

f.) Please provide details of where multi-factor authentication (MFA) is activated for all users:

☐ All systems and applications protected by MFA

☐ Remote access to the network (including Office 365 and remote desktop access) protected by MFA

☐ 3rd party bank applications protected by MFA

☐ Some systems and applications protected by MFA*

☐ No systems or applications protected by MFA*

*please provide further details of where and why MFA is not activated

g.) Do you or a managed service provider scan all incoming emails for malicious links and attachments?

Yes ☐ No ☐

h.) Please describe the process for dealing with emails that could cause potential security risks?

i.a.) Do you use any End-of-Life or unsupported systems or software, including those operating on an extended support basis? Yes ☐ No ☐

i.b.) Do you rely on any vendor's technical support for any software or hardware which has expired, been withdrawn, or is no longer available? Yes ☐ No ☐

If 'yes' to i.a) or i.b.) above:

i.i.) Are they used for critical processes or operations? Yes ☐ No ☐

i.ii) are they segregated from the rest of the network? Yes ☐ No ☐

i.iii) Please confirm any decommissioning plans or further protection or mitigation measures taken:

j.) 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 ☐

k.) 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, and prohibition of previously used passwords)? Yes ☐ No ☐

l.) 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 ☐

m.) Do procedures exist to operationalize 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 ☐

n.) Is personal information collected or stored on your network, systems or databases encrypted while at rest? Yes ☐ No ☐

If 'no' please provide details of how unauthorized access to data is prevented

o.) Do you publish any blogs, newsletters, videos, podcasts or other similar publications? Yes ☐ No ☐

If 'yes', are reviews (either internally or externally) always sought prior to the publication of new content? Yes ☐ No ☐

Section 5: Additional Coverages

Important note: Depending on the answers to the following questions and the Insurer selected these coverages may or **may not** be available.

Payment Card Industry (PCI) Data Security Standards (DSS) Cover

a.) Are you subject to Payment Card Industry (PCI) security standards? Yes ☐ No ☐

If 'yes' please indicate your merchant level

☐ 1
☐ 2
☐ 3
☐ 4

b.) Do you outsource all storing and processing of credit card information to a third party that accepts full responsibility for PCI compliance?

Yes ☐ No ☐

c.) If 'no' to question b.) have you been certified as being PCI compliant within the last 12 months or have you successfully completed a self-assessment audit? Yes ☐ No ☐

Cyber Crime Cover

a.) Do you verify new customer or supplier bank account information (including name, address and bank account number) prior to initiating any financial transaction with such supplier or customer?

Yes ☐ No ☐

b.) Do at least two members of staff review and authorize any transfer or funds, signing of cheques (above $10,000) or for the issuance of instructions for the disbursement of assets, funds or investments, which includes maintaining the sign-off documentation for your records? Yes ☐ No ☐

c.) Do you upon receipt of any email requests to change supplier or customer bank account details (including account number, email address, contact information, bank routing number):

i.) Have direct call back procedures in place (i.e. other than responding via email) to the contact number in place prior to receipt of the change request Yes ☐ No ☐

ii.) Require internal dual sign-off from a supervisor or authorized person prior to initiating the change request Yes ☐ No ☐

d.) If online banking software or systems are used to perform wire or banking transfer functions, is multi-factor authentication (MFA) activated for user log in and any transfers? Yes ☐ No ☐

For Professional service firms (including lawyers, accountants, etc.) and financial services only:

e.) Do you **always** verify with the requestor of a transfer, payment or delivery of funds, goods or services, the authenticity/validity of the request, via a method other than the original means of that request and maintain documentation to evidence the process with respect to:

i. Customer/Client/Vendor/Supplier instructions to direct funds, goods or services to a third party recipient;

AND

ii. Transactions or instructions where customer/client/Vendor/supplier account details vary from the account information held on record; **AND**

iii. Non-Standard requests made by senior management* for the transfer of funds, goods or services.

Yes ☐ No ☐

**** senior management** means 1) past, present and future duly elected or appointed director, officer, trustee or governor of a corporation, management committee member of a joint venture and member of the management board of a limited liability company or equivalent position including a de facto director, officer, trustee, governor, management committee member or member of the management board of such entities; and 2) past, present and future General Counsel and Risk Manager (or equivalent position) of you.*

Reputation Harm Cover

a.) Do you have more than 20% of your revenue coming from one customer or accounted for in one month during the past 12 months, or next 12 months (forecasted)? Yes ☐ No ☐

If 'Yes' to question a.) please provide further details.

Section 6: Claims/Incident History

a.) Are you aware of any circumstances or complaints against you in relation to data protection or security, or any actual security violations or security breaches either currently or in the past five years?

Yes ☐ No ☐

If 'yes' please provide further details

b.) Have you suffered any claim, loss or had any penalties/fines levied against you in the past five years in relation to the risks that this questionnaire relates to?

Yes ☐ No ☐

If 'yes' please provide further details

Declaration:

I/We hereby declare that:

My/Our attention has been drawn to the Important Notice on page 1 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**
	/ /		/ /

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.