AUSTBROKERS CYBER PRO

Cyber Insurance Corporate Proposal Form

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 Information to provide as part of your cyber insurance submission

Please provide the following information, if avaliable in support of your cyber insurance submission.

- **The Organisation's latest business continuity/disaster recovery or incident response plan.**
- **Any documentation in relation to cyber security standards and frameworks the organisation adheres to, i.e. Essential 8, ISO 27001, NIST etc.**
- **The latest vulnerability and/or penetration testing reports, including information on remediation that has taken place following such testing.**
- **Any other relevant information and material that will assist in demonstrating that your organisation has a strong level of cyber hygiene.**

Section 1: General 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

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

b.) Is your business a subsidiary, franchisee, or smaller entity of a larger organisation?

□ Yes, please provide further details

□ No

c.) Primary address (address, state, postcode, country)

d.) Description of Business operations

e.) Website address

f.) Primary Contact Details (Name, Telephone and email)

g.) When was your business established?

h.) Number of employees

i.) 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			

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

NSW	VIC	QLD	SA	TAS	ACT	NT	WA	O/S

Section 2: Data & Information Security

a.) 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?

□ Yes

□ No

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

b.) Approximately how many Individual's records have you collected and stored on your network? (Multiple pieces of information on the same individual can be considered as one record)

c.) Please tick the applicable boxes below in relation to the type of Personally Identifiable Information ('PII') that you collect, process and store.

□ Business & Customer Information (names, addresses etc)

□ Health Care Information (including medical records)

□ Financial Information (including bank account information)

□ Credit Card Information (including payment card numbers)

□ Tax File Numbers (including social security numbers)

□ Corporate Information (including intellectual property and trade secrets)

□ Biometric Information (including fingerprints and facial recognition)

d.) Do you share Personally Identifiable Information ('PII') with business partners, vendors or other parties?

□ Yes

□ No

If 'yes' please provide further details below.

e.) Please tick the applicable boxes below in relation to how Personally Identifiable Information ('PII') is protected within your network.

□ Restrict access to only those users required to have such access as part of their role

□ Regularly review authorisation access within the organisation (at least quarterly)

□ Timely removal of user access should access no longer be required for an individual (i.e. employee termination, job change etc)

□ Segmentation of PII within the network

□ Encryption of PII at rest

□ Encryption of PII in transit

□ Encryption of PII stored on portable media devices (including laptops and tablets).

f.) Does a formal policy exist regarding the disposal and/or purging of PII that is no longer required to be held by the organisation?

□ Yes

□ No

If 'no' please describe how you address this situation to ensure that PII that is no longer required to be kept is disposed of correctly

Section 3: Governance & IT Infrastructure

a.) Do you have a senior executive responsible for information security and management within the organisation, i.e., CIO etc?

□ Yes

□ No

b.) Please describe from a Board level the oversight the Board has in relation to cyber security, i.e., forms part of the board agenda, receives reports on new threats, engages regularly with CTO,CIO etc.

c.) Please describe any cyber security frameworks or best practices that have been adopted by the organisation, for example, Essential Eight, ISO 27001, NIST, PCI DSS

d.) What is your annual IT budget (approximately)?

e.) What approximate percentage of your IT budget is spent on IT security?

f.) Do you outsource any functions of your IT infrastructure to third parties (this may include a managed service provider and/or third parties providing cloud services, data hosting, data back up and storage, data processing etc)?

□ Yes

□ No

If 'yes' please list below your critical third-party technology providers, including a brief summary of the technology services they provide to you.

g.) Please describe the vetting procedures undertaken when engaging third party technology providers, including any review of their security and data protection controls.

h.) Does the organisation have a Secuirty Operations Centre ('SOC') that is responsible for monitoring and detection, vulnerability management and incident response?

□ Yes

□ No

If 'yes' please confirm details on the hours of operations (i.e. is it 24/7) and whether this is an internal function or outsourced to a third party (and who that third party provider is).

Section 4: Disaster Recovery & Back Ups

a.) Do you have a Business Continuity and/or Disaster Recovery and/or Incident Response Plan that addresses cyber risk and is it tested at least annually?

□ Yes

□ No

b.) Do you have a ransomware playbook, or have you conducted ransomware tabletop exercises at a Board level within the last 12 months?

□ Yes

□ No

If 'no' what policies and procedures exist within the organisation in relation to dealing with and handling a ransomware event?

c.) Please confirm the Recovery Time Objectives ('RTO') for critical systems:

□ 0-12 Hours

□ 12-24 Hours

□ 24 Hours + *(please provide further information here)*

d.) Please tick the applicable boxes below in relation to the technologies and protections used in relation to the organisation's backups.

□ Immutable or Write Once Read Many (WORM) technology

□ Offline/Air-gapped back ups disconnected from the rest of the network

□ Restricted access via separate privileged accounts

□ Multi Factor Authentication ('MFA') is enabled for access

□ Encryption of backups

□ Access to backups is logged and alerts for suspicious activity are configured and sent to the security team

□ Cloud hosted backups segmented from your network e.) Please tick the applicable boxes below in relation to the types of data backed up

- □ Critical Data Only
- □ Infrastructure (Operating systems and device configuration)
- □ Applications
- □ All of the above

f.) How often does backup testing/restoration take place (including confirming the integrity of the backups)?

- □ Quarterly or more regularly
- □ Bi annually
- □ Annually
- □ Other - *please provide further information here*

g.) How frequently are backups made to offsite storage?

- □ Quarterly or more regularly
- □ Bi annually
- □ Annually
- □ Other - *please provide further information here*

Section 5: Cyber Security Controls

a.) Do you have an Endpoint Protection Platform ('EPP') across your organisation?

- □ Yes
- □ No

If 'Yes', Does your Endpoint Protection have Detect and Respond (EDR) capabilities enabled?

- □ Yes
- □ No

Please also confirm which vendor is used

If the preceding is not on all endpoints, what percentage of endpoints do they apply to?

- □ 0–20%
- □ 21–50%
- □ 51–75%
- □ 76–99%

b.) Do you have firewall technology deployed at all network points and do formal (e.g. not default) firewall configurations exist?

- □ Yes
- □ No

c.) 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

d.) Do you have a policy/process in place to deploy critical patches within 14 days?

□ Yes

□ No

If 'no' please describe your patch management policy and timelines around the deployment of critical patches

e.) Are external vulnerability scans and/or penetration tests conducted on at least an annual basis, with any vulnerabilities identified and remediated?

□ Yes, *please provide details of the third party provider conducting such test below*

□ No, *please describe other measures in place to identify vulnerabilities within the network below*

f.) Do you allow remote access into your network?

□ Yes

□ No

If 'yes' please tick the applicable boxes that apply in relation to securing such remote access into your network

□ Use of Remote Desktop Protocol (RDP)

□ Use of a Virtual private Network (VPN)

□ Multi Factor Authentication is enabled

□ Single Sign On (SSO) via MFA

□ Please list any other security controls used to protect remote access into the network

g.) Please tick the applicable boxes below that apply to securing email activity within the organisation

□ MFA is required for webmail and cloud based email accounts

□ Advanced Threat Protection (ATP) enabled

□ Sender Policy Framework (SPF) is enforced

□ Secure email gateway is enforced

□ All incoming emails are scanned for malicious links and attachments

□ Any suspicious emails are automatically quarantined

□ Microsoft Office macros are disabled by default

□ Domain Keys Identified Mail (DKIM) is enforced

□ Sandboxing is used for investigating email attachments

□ Please list any other controls in place in relation to securing email activity

h.) Please tick the applicable boxes that apply to securing privileged accounts within the organisation (please note, privileged accounts are those accounts that provide administrative or specialised levels of access based on a higher level of permission).

□ Multi-Factor Authentication (MFA) for all privileged access or administrator accounts in place

□ The use of unique credentials for certain administrative tasks

□ Access logs are stored for at least 90 days

□ Principle of Least Privilege (POLP) in place

□ Privileges Access Management (PAM) tool in place

□ Privileged accounts and directory services are monitored for unusual activity

□ Privileged access workstations (workstations that do not have access to the internet or emails) are used for the administration of critical systems

i.) Do you operate any end of life or unsupported hardware, software or systems?

□ Yes

□ No

If 'yes' please outline what these are, what they are used for and your plans and timelines around decommissioning or upgrading such systems

j.) Is any of this hardware, software, or systems in question 'i.)' business critical?

□ Yes

□ No

Are these systems segregated and isolated from the rest of the network (including restricted from internet access)?

□ Yes

□ No

k.) Does the organisation have Data Loss Protection software across its network?

□ Yes

□ No

If 'no' please describe how the organisation detects and prevents exfiltration of data from its network l.) Please describe how the organisation limits lateral movement within its network (this may include segmenting networks between geography/business functions).

m.) How frequently do you conduct the following training for all employees?

Cyber Risk Awareness Training

- □ Never
- □ Annually
- □ Bi Annually
- □ Quarterly
- □ Monthly

Phishing Email Simulations

- □ Never
- □ Annually
- □ Bi Annually
- □ Quarterly
- □ Monthly

Do you require additional training for employees who fail phishing email simulations?

- □ Yes
- □ No

Section 6: Media

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

- □ Yes
- □ No

If 'yes' are reviews (either internally or externally) conducted prior to the publication of such content?

- □ *Yes*
- □ *No*

b.) Does the organisation have a policy in relation to the use of social media?

- □ Yes
- □ No

If 'no' please outline the process and controls in place in relation to posting content on social media

Section 7: Claims/Incident History

a.) Are you aware of any claims, circumstances or complaints against you in relation to a data breach, security breach, cyber incident or violations of privacy regulations?

□ Yes

□ No

If 'yes' please provide further details including the date of the incident, a description of the incident, any financial costs associated with the incident and risk mitigation processes and controls put in place since the incident?

b.) Has the organisation or any of its directors or officers been subject to an investigation by a regulator in relation to privacy or security matters (regulators may include the OAIC, ASIC, APRA etc)?

□ Yes

□ No

If 'yes' please provide further details including the date of the investigation, a description of the investigation, any financial costs associated with the investigation (including any fines and penalties) and risk mitigation processes and controls put in place since the investigation

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 context by my/our signature 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 authorize INSURERS to collect or disclose any personal information relation to this insurance to/from any other insurers or insurance reference services. 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 entitles 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/CIO or equivalent/Principal of the association/Partnership/Company/Practices/Business

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.