Austbrokers Info Tech

Combined Technology Insurance Proposal Form

Statutory 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 available 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. Essential8, 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.

Scanning Tools

As part of providing your cyber insurance submission to Austbrokers Info Tech, we engage with third parties which may use tools to scan external elements of your IT infrastructure and networks in order to identify potential risks and vulnerabilities.

Important Information:

- 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 provide a separate attachment on your company letter-head.

Section 1: General Information

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

b.) Is your business a subsidiary, franchisee, or smaller entity of a larger organisation? ☐ **Yes** ☐ **No**

If 'no', please proceed to question c.) below, If Yes, please answer the following:

- Please provide details of the franchisor or larger organisation
- Is there any system connectivity with the entity which you are a subsidiary or franchisee of? ☐ **Yes** ☐ **No**
- Do you share any data with an entity that you are a subsidiary or franchisee of? ☐ **Yes** ☐ **No**
- Does the entity which you are a subsidiary or franchisee of hold insurance policies which are entitled to claim under? ☐ **Yes** ☐ **No**

c.) Has your business merged or purchased another business in the last 3 years? ☐ **Yes** ☐ **No**

If 'yes' please provide details below:

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

e.) Website address:

f.) When was your business established?

g.) Number of employees:

h.) Please provide revenue details as per below

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

i.) If you generate revenue from the USA or Canada do you have a registered business premises based in these jurisdictions? ☐ **Yes** ☐ **No**

If 'no' to the above, how do you support overseas work? i.e. visiting staff, contractors, remote communication methods etc.

j.) Over the past 4 years, how many years did you post a positive net income position?

☐ 0 ☐ 1 Years ☐ 2 Years

☐ 3 Years ☐ 4 Years

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

NSW	VIC	QLD	SA	TAS	ACT	NT	WA	Overseas

Technology/Professional Liability

Section 2 – Business Activity

a.) Please provide a description of your business activities

b.) Please provide an approximate percentage of your turnover from each of the following activities undertaken:

1.Hardware Seller – Own Products	1.
2.Hardware Seller – Third Party Products	2.
3.Hardware or peripheral maintenance	3.
4.Software developer/sales – applications, custom, bespoke	4.

5.Software developer/sales – shrinkwrap prepackaging	5.
6.Software developer/sales – control systems	6.
7.Software developer/sales – standard	7.
8.Software support and maintenance	8.
9.Manufacture own products & Hardware Assembly	9.
10.Artificial Intelligence	10.
11.VAR and retail sales	11.
12.Systems integration (incl. ERP / CRM / SAP)	12.
13.Payment processing systems	13.
14.Application Service Provider (ASP)	14.
15.Internet security product or service providers	15.
16.Managed service provider	16.
17.Internet Service Provider (ISP)	17.
18.Cyber Security Consultancy	18.
19.Consultancy / miscellaneous IT services	19.
20.Website development / graphic design	20.
21.Broadcasting/Streaming	21.
22.Education and training	22.
23.IT Recruitment services	23.
24.Business analysis / project management	24.
25.Data warehousing	25.
26.Facilities management / outsourcing services / hosting / cloud services	26.
27.Support, call centre or help desk	27.
28.Telecom carriage services	28.
29.Other (not specified above, please specify):	29.

c.) Do you use sub-contractors to perform any of the above services? ☐ Yes ☐ No

If 'no', please proceed to question g.), If Yes, please answer the following:

d.) Do you require sub-contractors to carry:

- Professional Indemnity Insurance ☐ Yes ☐ No
- Public and Products Liability Insurance ☐ Yes ☐ No

e.) Do you maintain full subrogation rights against your sub-contractors? ☐ Yes ☐ No

f.) Please select vetting processes in place for sub-contractors:

☐ Skills registers for licensing ☐ Experience in the field ☐ Long term relationship
☐ Tender ☐ Other (please provide detail):

g.) Are your products, services or applications to customers used in the following industries? If Yes, please provide an approximate percentage of turnover

			% of Turnover
Aerospace	☐ Yes	☐ **No**	%
Defence/Military Fire, security or other emergency	☐ Yes	☐ **No**	%
Industrial control systems, Process control systems, SCADA, PLC	☐ Yes	☐ **No**	%
Medical/healthcare industry	☐ Yes	☐ **No**	%
Mining	☐ Yes	☐ **No**	%
Oil, gas, power, nuclear, energy	☐ Yes	☐ **No**	%
Transportation	☐ Yes	☐ **No**	%
Social Media	☐ Yes	☐ **No**	%
Technology security services	☐ Yes	☐ **No**	%
Financial services trading platforms including gambling	☐ Yes	☐ **No**	%

h.) Please select the likely result of a failure of your products or services or delay in their implementation? (tick all that are relevant)

☐ Loss of life or injury ☐ Immediate and large financial loss ☐ Insignificant Loss
☐ Significant cumulative financial loss ☐ Damage or destruction of property

i.) Are legal counsel consulted prior to release of all new products? ☐ **Yes** ☐ **No**

j.) What percentage of your revenue is derived from products that are:

☐ 1 year old or less ☐ 1-2 years old ☐ 3 years old or more

Section 3: Contract Information

a.) Please provide details of your five largest contracts

Customer Name	Nature of Product/ Service	Total Contract Value	Contract Duration	Development Duration	Deployment Duration	Maintenance Duration
1.	1.	1.$	1.	1.	1.	1.
2.	2.	2.$	2.	2.	2.	2.
3.	3.	3.$	3.	3.	3.	3.
4.	4.	4.$	4.	4.	4.	4.
5.	5.	5.$	5.	5.	5.	5.

b.) What is your average contract value? $

c.) What is your average contract duration?

d.) Are any government contracts in excess of $500,000 or 18 months duration? ☐ **N/A** ☐ **Yes** ☐ **No**

If 'yes' please provide full scope of services provided below including contract value, contract period etc:

e.) Are your privacy policy, terms of use, terms of services and other customer contracts drafted reviewed by legal professionals? ☐ **Yes** ☐ **No**

f.) Do you always have a written contract in place with your customers and specifies scope of services? ☐ **Yes** ☐ **No**

If 'no' to question f.) above, please provide further details on risk management.

g.) How often do you use your own standard terms and conditions contracts? %

h.) What percentage of your customer contracts, purchase orders or user agreements contain:

- Hold harmless or indemnity agreements insuring the benefit of You? ☐ Less than 50% ☐ More than 50%
- Hold harmless or indemnity agreements insuring to the benefit of the customers? ☐ Less than 50% ☐ More than 50%
- Statement of Work ☐ Less than 50% ☐ More than 50%
- Exclusion of consequential damage ☐ Less than 50% ☐ More than 50%
- Liquidated Damages provisions ☐ Less than 50% ☐ More than 50%
- Dispute resolution process ☐ Less than 50% ☐ More than 50%
- Limitation of liability provisions that extend to actual or alleged breach of sensitive PII. ☐ Less than 50% ☐ More than 50%

i.) Are all variations from the initial scope of works documented in writing? ☐ **Yes** ☐ **No**

j.) Is there a formal acceptance process with your customer for any scope of work variations and on delivery of your products and services? ☐ Yes ☐ No

Section 4: Quality Control and Systems Development Management

a.) Do you have written quality management systems or procedures in place? ☐ Yes ☐ No

b.) Do you have procedures in place for documenting problems, downtime and responses to customer complaints/feedback? ☐ Yes ☐ No

c.) Do you have systems development methodology in writing for custom software development and system integration projects? ☐ Yes ☐ No

If 'no', to question b.) or c.) above, please provide details on what procedures are in place.

If you manufacture, or you have a third-party manufacture on your behalf, please complete the following:

d.) Do you or your third-party manufacture have quality control procedures in place such as:

- Formalised written quality control plans? ☐ Yes ☐ No
- Production design sign off acceptance and sign off procedures for statements of work or contracts? ☐ Yes ☐ No
- Prototype development protocols ☐ Yes ☐ No
- Batch testing ☐ Yes ☐ No

Section 5: Intellectual Property and Media

a.) Do you hold any patents or any patent applications pending? ☐ Yes ☐ No

b.) Who reviews content prior to publishing via any media (including website, social networking or printed media)?

c.) Do your intellectual property or compliance procedures include the following:

- Formal procedures to safeguard against Infringement of others intellectual property rights ☐ Yes ☐ No
- Searches conducted for all trademark, copyright or patent applications ☐ Yes ☐ No
- Libel or slander Reviews ☐ Yes ☐ No
- Procedures in place to secure rights for using third party content via any media stream ☐ Yes ☐ No

Section 6: Technology/Professional Liability Claims

a.) After enquiry of the Partners/Principals/Directors and employees, is there any circumstances or is there a pending claim against the Proposed Insured, its Subsidiaries, it's predecessors in business or its current or former Partners/ Principals/Directors or employees for a Civil Liability in the performance of the Proposed Insured's information technology Services/products? ☐ 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.) After enquiry of the Partners/Principals/Directors and employees, is the Proposed Insured or any of its Subsidiaries aware of any prosecution or investigation (actual or pending) of the Proposed Insured, any Subsidiary, or any Partner / Principal/Director or employees under any International, Commonwealth, State or Local statute, legislation, regulation or By Law?

☐ **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?

Cyber Security

Section 1: Data and 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.) Please tick the applicable boxes 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)

c.) 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)?

d.) Please tick the applicable boxes 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).

Section 2: Recovery and Backups

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**

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

b.) Do you have a ransomware playbook, or have you conducted ransomware tabletop exercises with employees and at a Board level within the last 12 months? ☐ ***Yes*** ☐ ***No***

c.) 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

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

☐ 0-12 Hours ☐ 12-24 Hours ☐ 24 Hours + (please provide further information below)

e.) 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 below)*

f.) Do you operate any end of life or unsupported hardware, software or systems? ☐ Yes ☐ No

g.) Is any of this hardware, software, or systems in question 'f.)' business critical? ☐ Yes ☐ No

h.) Are these systems segregated and isolated from the rest of the network (including restricted from internet access)? ☐ Yes ☐ No

i.) If 'yes' to any of the above please outline timelines around decommissioning or upgrading such systems

Section 3: Cyber Security Controls

a.) Which of the following have you (or your provider, if outsourced) implemented to help protect information and systems from a Data Breach or a Cyber Incident?

- Dedicated staff member governing data and IT ☐ Yes ☐ No
- Formal privacy policy approval by legal counsel ☐ Yes ☐ No
- Ongoing staff training on privacy and security related matters including ransomware and phishing email stimulations ☐ Yes ☐ No
- Data retention Plan ☐ Yes ☐ No
- Bring Your Own Device (BYOD) plan ☐ Yes ☐ No
- Firewalls at all external connection points ☐ Yes ☐ No
- Antivirus across all networks ☐ Yes ☐ No
- Vulnerability assessments/penetration tests ☐ Yes ☐ No
- Software updated and patching procedures in place with critical patches deployed within 14 days. ☐ Yes ☐ No
- Advanced Endpoint Protection with detect and respond (EDR) capabilities enabled ☐ Yes ☐ No
- Intrusion Detection Systems ☐ Yes ☐ No
- Encryption of data in transmission ☐ Yes ☐ No
- Encryption of data at rest and in backups ☐ Yes ☐ No
- Password protocols i.e. password length, regularly changed ☐ Yes ☐ No
- Multi-factor authentication for:

☐ Remote Access ☐ Backups ☐ Privileged access of administration accounts

☐ Cloud resources (including office365) ☐ Virtual Desktop Instances

Please provide further details on any further cyber security controls:

b.) 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) enables

- ☐ 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 investigation email attachments

c.) 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 specialized 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
- ☐ Privileged 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

Section 4: Cyber 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 authorized 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.