Codex TechShield
Proposal Form

codexinsurance.com

‹ Ensuring our Future ›

*Please read the **'Important Notices and Statements'** on pages 11-13 before completing this form.*

PART 1. General Information

Insured name

Principal address

Year Established **ABN** **Website**

PART 2. Operational Information

2.1 Is your entity a subsidiary of another entity? Yes ☐ No ☐

2.2 Within the past five years, have you participated or been the subject of any mergers or acquisitions? Yes ☐ No ☐

2.3 Have you participated in any joint ventures within the past five years? Yes ☐ No ☐

2.4 Do you envision any material changes in ownership or operations that may take place over the next twelve months? Yes ☐ No ☐

If yes to any of the above questions, please provide further details.

2.5 Please provide the total number of employees (including principals/directors):

2.6 Please provide your total gross revenue (including contractor payments) per region:

	Australia	**Overseas (excl. USA)**	**USA**	**Total**
Prior 12 months	$	$	$	$
Current 12 months	$	$	$	$
Next 12 months	$	$	$	$

2.7 Please provide a percentage breakdown of total gross revenue (including contractor payments) which are attributable to the following jurisdictions:

NSW	QLD	VIC	TAS	SA	WA	ACT	NT	Overseas	**Total**
%	%	%	%	%	%	%	%	%	**100 %**

2.8 Please select the total number of unique records stored containing Personal Information.

☐ 0-10,000 ☐ 50,001-75,000 ☐ 200,001-300,000 ☐ 500,001-750,000

☐ 10,001-25,000 ☐ 75,001-100,000 ☐ 300,001-400,000 ☐ 750,001-1,000,000

☐ 25,001-50,000 ☐ 100,001-200,000 ☐ 400,001-500,000 ☐ >1,000,000

** Personal Information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.*

2.9 Please indicate whether the following types of data and/or information are being collected, stored, processed, transmitted and/or secured by or on behalf of your entity:

a) Personal data (e.g. full name, address, date of birth, etc) Yes ☐ No ☐

b) Sensitive personal data (e.g racial or ethnic origin, political views, religious beliefs, sexual orientation, criminal history, etc) Yes ☐ No ☐

c) Driver licence or passport numbers Yes ☐ No ☐

d) Tax File Numbers (TFNs) Yes ☐ No ☐

e) Payment card information Yes ☐ No ☐

f) Financial account information Yes ☐ No ☐

g) Classified third party trade secrets or intellectual property Yes ☐ No ☐

h) Healthcare/medical records (including Medicare numbers) Yes ☐ No ☐

2.10. Are you required to comply with the latest Payment Card Industry Data Security Standard (PCI DSS)? If yes, please specify the PCI DSS merchant level that applies to your business:

☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4 ☐ Not applicable

PART 3. Activity Information

3.1 Please provide a complete description of all the activities conducted by your entity:

3.2 Do you undertake any activities relating to:

a) Adult entertainment

b) Aerospace or aviation

c) Maritime

d) Critical infrastructure (e.g. utilities, broadband, telecommunication)

e) Cryptocurrencies, tokens or blockchain protocols

f) Gambling or other games of chance

g) Oil and gas

h) Satellite communications

i) Transportation and logistics

j) Auction platforms

k) Financial payment, trading or insurance systems/platforms

l) Credit or background screening and verification systems

m) Manufacture of Internet of Things (IoT) devices

n) Manufacture of components for safety critical systems

o) Data wholesaling or broking

p) Social media platforms

Yes ☐ No ☐ If yes, please provide further details below:

3.3 Please provide a percentage breakdown of total gross revenue for each activity:

Activity	Percentage
Software reselling (third-party developed)	%
Software selling and licensing (self-developed)	%
Hardware reselling (third-party developed)	%
Hardware design and manufacture	%
Computer hardware assembly	%
Installation, configuration and maintenance of hardware or software	%
Custom software application design and development	%
Website design and development	%
Website hosting	%
Data analysis	%
Data warehousing	%
IT consulting	%
System integration	%
Helpdesk and IT support	%
IT project management	%
IT education and training	%
IT employment placement and recruitment	%
Digital marketing (including Search Engine Optimisation (SEO))	%
Subscription based Software as a Service (SaaS) provider	%
Digital marketplace platform provider	%
Cloud hosting, computing and migration services	%
Managed cloud, network and security services	%
Communications Service Provider (CSP)	%
Business Process Outsourcing (BPO)	%
Other (please specify)	%
Total	**100 %**

3.4 Do you undertake any manufacturing, construction, erection or installation activities? Yes ☐ No ☐

If yes, please provide please a description of the activity and state the percentage of total gross revenue declared that relates to such activities.

Activity	Percentage
	%

3.5 Do you engage consultants, contractors, labour-hire personnel or agents to perform any services or activities on your behalf? Yes ☐ No ☐

If yes:

a) Please specify the percentage of total gross revenue paid to such entities collectively over the past 12 months. %

b) Please provide a complete description of all services and activities that are contracted-out or outsourced.

c) Are these entities contractually required to effect and maintain minimum levels of relevant insurance cover? Yes ☐ No ☐

3.6 Please provide details in relation to your three largest contracts/projects:

Client Name	Services/Products	Project Value	Fees Earned	Duration
		$	$	
		$	$	
		$	$	

3.7 Please select your Maximum Tolerable Downtime (MTD) with respect to your most mission-critical application or system.

☐ Immediate ☐ 12 hours ☐ 48 hours ☐ 96 hours

☐ 8 hours ☐ 24 hours ☐ 72 hours ☐ 120 hours

PART 4. Quality Assurance and Controls

4.1 Do you have a formalised quality assurance and control programme? Yes ☐ No ☐

4.2 Please confirm if you have the following quality control procedures in place:

a) Performance milestone and final deliverable acceptance and sign-off procedures

Yes ☐ No ☐ Not applicable ☐

b) Incident logging, response and post-mortem review protocols (e.g. incident register)

Yes ☐ No ☐ Not applicable ☐

c) Complaints handling and dispute resolution procedures

Yes ☐ No ☐ Not applicable ☐

d) Continuous support, maintenance and patch management protocols

Yes ☐ No ☐ Not applicable ☐

PART 5. Contractual Risk Management

5.1 Do you always have written agreements in place with your clients? Yes ☐ No ☐

5.2 What percentage of your total contracts have been issued and accepted on your standard contract terms and conditions? %

5.3 Have your standard contract terms and conditions been reviewed by a legal professional? Yes ☐ No ☐

5.4 Do you have a formalised change control procedure in place to address amendments to any Scope/Statement of Work (SoW) previously agreed upon? Yes ☐ No ☐

5.5 Do all your terms and conditions or contracts contain a limitation of liability clause which expressly excludes consequential loss (apart from intellectual property or confidentiality clauses) to the fullest extent permissible by law? Yes ☐ No ☐

If no, how do you limit your liability in such circumstances?

5.6 Do you ever agree to indemnify or hold harmless any third party for claims arising out of your services or products? Yes ☐ No ☐

5.7 Are all non-standard contracts (including variations to standard contract terms) required to be reviewed by a legal professional and approved by senior management prior to acceptance? Yes ☐ No ☐

PART 6. Intellectual Property Protocols

6.1 Do you own any registered trademarks, patents or copyrights? Yes ☐ No ☐

If yes, please answer the following series of questions:

a) Do you always obtain and adhere to the legal advice and recommendations of a qualified patent attorney before releasing any new software and/or products to the public? Yes ☐ No ☐

b) Do you have formalised search and clearance protocols in place for all trademarks, copyright and patent applications? Yes ☐ No ☐

PART 7. Cybersecurity Governance and Controls

7.1 Does a documented baseline security framework exist across all operations, entities, subsidiaries including international locations? Yes ☐ No ☐

7.2 Does a documented asset inventory exist, which categorises all systems, software and data by level of sensitivity or criticality? Yes ☐ No ☐

7.3 Do you have an incident response plan which addresses network incidents and data breaches? Yes ☐ No ☐

If yes, has the incident response plan been tested in the past 12 months? Yes ☐ No ☐

7.4 Do you conduct periodic vulnerability assessments/penetration tests? Yes ☐ No ☐

7.5 Is Personal Information encrypted whilst:

a) In transit Yes ☐ No ☐

b) At rest Yes ☐ No ☐

c) On portable or removable devices Yes ☐ No ☐

7.6 Do you pre-screen emails for malicious attachments and links? Yes ☐ No ☐

7.7 Do you enforce email authentication controls (SPF, DKIM, and DMARC) on incoming email? Yes ☐ No ☐

7.8 Do you regularly (at least annually) provide cyber security awareness training, including social engineering and anti-phishing, to all staff who have access to your organisation's network or confidential/personal data? Yes ☐ No ☐

7.9 Do you require Multi-Factor Authentication (MFA) for remote access to your network (both cloud-hosted and on-premises, including via Virtual Private Networks (VPNs)) including access to any web-based email? Yes ☐ No ☐

7.10 Do you use Office 365 in your Organisation? Yes ☐ No ☐

If yes, do you use the Microsoft Defender add-on, or similar alternative product? Yes ☐ No ☐

7.11 What security solutions do you use to prevent or detect malicious activity on your network?

☐ Endpoint Protection Platform (EPP) ☐ Endpoint Detection and Response (EDR) ☐ Managed Detection and Response (MDR)

7.12 Is event logging implemented across your enterprise environment? Yes ☐ No ☐

7.13 Do you use MFA to protect privileged accounts? Yes ☐ No ☐

7.14 Do you use a hardened baseline configuration across all (or substantially all) of your devices? Yes ☐ No ☐

7.15 In what time frame do you install critical and high severity patches across your enterprise once received?

☐ 24 hours ☐ 48-72 hours ☐ 7 days ☐ 1 month ☐ >1 month

7.16 Have you configured host-based and network firewalls to disallow inbound connections by default, unless they are explicitly required for operational purposes? Yes ☐ No ☐

7.17 Do you use a protective DNS service (e.g Quad9, OpenDNS or PDNS)? Yes ☐ No ☐

7.18 Do you permit ordinary users local administrator rights to their devices (e.g. laptops)? Yes ☐ No ☐

7.19 Do you disable macros in your office productivity software (e.g. Microsoft Office, Google Workspace) by default? Yes ☐ No ☐

7.20 Do you provide your users with password manager software? Yes ☐ No ☐

7.21 Do you manage privileged accounts using tooling (e.g CyberArk)? Yes ☐ No ☐

7.22 Do you have any end-of-life or end-of-support software on your network? Yes ☐ No ☐

If yes, what mitigating controls do you enforce on such software?

☐ Segregation/DMZ ☐ No internet connection ☐ Outbound connection only

PART 8. Back-up and Redundancy Procedures

8.1 How regularly do you back-up your business-critical data?

☐ At least daily ☐ At least weekly ☐ At least monthly ☐ Rarely/never

8.2 Are your back-ups always encrypted? Yes ☐ No ☐

8.3 Where do you back-up your business-critical data?

☐ Internal network ☐ Cloud service ☐ Offline

8.4 If you rely on a cloud-based back-up service, is it a “syncing service” (e.g Dropbox, OneDrive, Google Drive)?

☐ Yes ☐ No ☐ Not applicable

8.5 How frequently do you perform a test restoration from back-ups?

☐ Quarterly or more ☐ 2-3 times per year ☐ Annually ☐ Rarely/never

8.6 Is access to back-ups restricted to dedicated privileged accounts not used for any other function? Yes ☐ No ☐

8.7 Have you provisioned sufficient network bandwidth to restore large cloud back-ups within your Recovery Time Objective (RTO)? Yes ☐ No ☐

8.8 Which of the following best describes your current system hosting arrangement?

☐ Fully hosted on internal infrastructure ☐ Partially hosted on internal and third-party infrastructure ☐ Fully hosted by a third-party provider

8.9 What high availability or redundancy provisions are currently in place for your mission-critical systems?

☐ Geo-redundant Storage (GRS) ☐ Disk-level redundancy (RAID) ☐ Automatic failover/clustering ☐ Load-balancing

8.10 Have you implemented network segmentation and segregation to restrict and limit access to sensitive systems and datasets? Yes ☐ No ☐

PART 9. Optional Extension - Social Engineering Fraud

8.1 Do you require social engineering fraud cover? Yes ☐ No ☐

If yes, please specify your desired sub-limit and answer the following questions:

☐ $10,000 ☐ $25,000 ☐ $50,000 ☐ $100,000 ☐ $250,000

a) Are employees who are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise and other scams, on at least an annual basis? Yes ☐ No ☐

b) Are employees required to independently verify all requests to transfer funds over $5,000 through alternative communication channels with a pre-authorised contact for authenticity? Yes ☐ No ☐

c) When a vendor or supplier requests any change to its account details (including routing/account numbers), do you confirm requested changes via an out-of-band authentication (a method other than the original means of request)? For example, if a request is made by email, a follow-up phone call is placed to confirm that the supplier or vendor made the request. Yes ☐ No ☐

PART 10. Claims and Loss History

9.1 Have you or any past or present principal, partner or director (including any prior business), employee, subsidiary or individual contractor:

a) been claimed against with respect to the coverage being sought? Yes ☐ No ☐

b) incurred any other loss or expense which might fall within the terms of cover being sought? Yes ☐ No ☐

9.2 After conducting an investigation, is any principal, partner, director, employee or individual contractor aware of any facts or circumstances that could:

a) potentially lead to a claim or inquiry against you, your predecessors in business, or any of the current or former partners, principals, directors, independent contractors or employees? Yes ☐ No ☐

b) result in you, your predecessors, or any of the current or former partners, directors, independent contractors, employees or principals incurring losses or expenses that might fall under the coverage being sought? Yes ☐ No ☐

c) otherwise impact the assessment of this insurance? Yes ☐ No ☐

9.3 After conducting a review, are you aware of any pre-existing vulnerabilities present within any system component listed as a Common Vulnerability and Exposure (a “CVE) in the National Vulnerability Database, where patches, fixes or mitigation techniques have been made available but have not yet been applied? Yes ☐ No ☐

PART 11. Insurance Coverage Details

10.1 Please specify limits, excesses and waiting periods required per section of coverage:

Coverage	Limit	Excess
Technology Professional Indemnity	$	$
Cyber Liability	$	$
Cyber Crisis Response Costs and Reimbursement	$	$
Public and Products Liability	$	$

10.2 Please provide details of your current insurance policies:

Coverage	Limit	Excess	Premium	Insurer	Retroactive Date
Tech E&O	$	$	$		
Cyber	$	$	$		
General Liability	$	$	$		

10.3 Has any insurance company, regarding the risks associated with this proposal, ever:

a) rejected a proposal, declined to renew, or terminated insurance? Yes ☐ No ☐

b) requested a higher premium or imposed special conditions? Yes ☐ No ☐

c) refused or reduced its obligation to fully pay an insurance claim? Yes ☐ No ☐

Declaration

I/we, the undersigned, hereby declare that:

1. I am/we are duly authorised to sign this Proposal Form and affirm that the statements provided are correct, true, and complete, with no material information withheld.
2. I/we confirm that I/we have reviewed and understood the important facts and advice related to the duty of disclosure and have diligently made all necessary inquiries to ensure compliance with this duty.
3. I/we acknowledge that no insurance will be in effect until the insurer confirms acceptance of the proposed insurance, and I/we undertake to inform the insurer of any material changes to the provided information before the insurance contract is finalised.
4. I/we understand that the insurer relies on the information and representations made in this Proposal Form and any related communications, and, unless stated otherwise, any statement made will be treated as applicable to all persons to be insured.
5. I/we have read and consent to Codex Insurance's Privacy Statement, agreeing to the collection, use, and disclosure of personal information as outlined therein.

Signature(s):

Name of Partner(s) or Director(s):

Date:

Important Notices and Statements

These are provided for your information only and do not form part of the insurance contract, nor do they impose any contractual obligations or grant any contractual rights.

Duty of Disclosure Statement

Prior to entering an insurance agreement, you have a responsibility to disclose any information that you know or ought to know that could impact our decision to insure you and the conditions under which we do so. This obligation remains in effect until we consent to insure you. The same duty applies when you renew, extend, modify, or reinstate an insurance contract.

You are not required to inform us of anything that decreases the risk we are insuring you for, is widely known, or should be known by us as an insurer, or if we have waived your obligation to inform us.

Failing to disclose necessary information may result in the termination of your contract or a reduction in the amount of compensation you receive if you file a claim, or both.

If your omission is intentional or fraudulent, we may refuse to honour a claim and invalidate the contract.

Agent of the Insurer

Codex Insurance Pty Ltd (ABN 40 669 032 811) ('Codex Insurance'), an Australian company and a Corporate Authorised Representative (CAR No. 1314764) of Insurance Advisernet (ABN 15 003 886 687, AFSL No. 240549), operates under an agreement with Certain Underwriters at Lloyd's of London (Lloyds), led by MS Amlin, Syndicate 2001, which provides it with the authority to effect insurance contracts, where Codex Insurance will be solely acting as an agent of Lloyds, and not acting on your behalf.

Claims Made and Statutory Notice

Parts of this policy are issued on a 'Claims Made' basis, which means that these sections only provide cover for claims made against the Insured during the period of insurance related to conduct that occurred, was attempted, or was alleged to have occurred or been attempted after the specified retroactive date mentioned in the schedule.

This excludes coverage for claims or potential claims that you were aware of before the period of insurance and that would have alerted a reasonable person in your position to the possibility of a claim being made against you. However, there may be some exceptions to this condition if a "Continuous Cover" extension is in place.

In accordance with Section 40(3) of the Insurance Contracts Act 1984 (Cth), if you become aware of any incident or information that may result in a claim against you by a third party during the period of insurance, you must notify us of the matter before the policy expires. Failure to notify us before the policy expires will result in the insured person losing the benefit of Section 40(3), and we may refuse to pay any subsequent claim, even if the events or circumstances leading to the claim occurred during the period of insurance. However, if the insured person complies with this section, we cannot refuse to indemnify them, even if no claim is made against them during the period of insurance.

Pursuant to Section 54 of the Insurance Contracts Act 1984 (Cth), if you report any claims made against you during the period of insurance (or automatic or extended reporting period, if applicable) after the expiration of the period of insurance or any relevant extended reporting period, we reserve the right to reduce our liability. This reduction will be based on a fair assessment of the degree to which our interests were adversely affected by the delay.

Subrogation Waiver

Our policy contains a provision that has the effect of excluding or limiting our liability in respect of a liability incurred solely by reason of the Insured entering into a deed or agreement excluding, limiting or delaying the legal rights of recovery against another.

General Insurance Code of Practice

We are committed to providing high-quality insurance products and services to our customers. As a signatory to the General Insurance Code of Practice (the Code), we are committed to upholding the standards set out in the Code. Access a copy of the Code at http://www.codeofpractice.com.au/ or alternatively, contact the Insurance Council of Australia on 9253 5100.

Privacy Statement

We are committed to protecting the privacy of your personal information. We comply with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) and other relevant legislation, which regulate the handling of personal information by organisations. This privacy statement describes how we collect, use, and protect the personal information you provide to us when you purchase an insurance policy with us. Please read carefully.

Collection of Personal Information

We may collect the following types of personal information from you:

- Contact details, such as your name, address, email address, and phone number.
- Financial information, such as your credit card or bank account information, and your income.
- Insurance-related information, such as your policy details, claims history, and medical information.
- Other information that you choose to provide to us, such as your preferences, feedback, or survey responses.
- We may collect this information from you directly, or from third parties, such as insurance brokers or other service providers.

Use of Personal Information

We use your personal information for the following purposes:

- To provide you with insurance services, including processing your application, managing your policy, and processing claims.
- To communicate with you, including providing you with information about your policy, sending you newsletters and other marketing materials, and responding to your inquiries and feedback.

- To improve our products and services, including conducting research and analysis, and developing new insurance products.
- To comply with legal and regulatory requirements, including anti-money laundering, fraud prevention, and other legal obligations.

Sharing of Personal Information

We may disclose your personal information to the following third parties:

- Service providers, such as claims adjusters, medical professionals, and other service providers who assist us in providing insurance services to you.
- Other insurance companies, reinsurers, and underwriters, who may need your information to provide you with coverage or assess risk.
- Regulatory authorities, law enforcement agencies, and other public bodies, when required by law or in response to legal requests.
- Other third parties with your consent.
- We take reasonable steps to ensure that these third parties comply with the APPs and other privacy requirements.

Storage and Security of Personal Information

We take reasonable steps to protect your personal information from unauthorised access, use, and disclosure. We maintain physical, technical, and administrative safeguards to protect your information. We store your personal information in secure electronic and physical locations, including cloud-based servers. We may store your personal information outside of Australia, and we take steps to ensure that such information is protected to a standard equivalent to the APPs.

Access to and Correction of Personal Information

You have the right to request access to, and correction of, your personal information that we hold. We will respond to your request as soon as practicable, and we may charge a reasonable fee for providing access. If we refuse to provide access or correct your personal information, we will provide you with a written notice explaining the reasons for refusal.

Changes to this Privacy Statement

We may update this privacy statement from time to time to reflect changes in our information practices. We will notify you of any material changes by posting the updated statement on our website or by other means.

Complaints and Contact Information

To obtain more details about our privacy practices, including accessing or modifying your personal information, filing a complaint, obtaining a list of foreign countries, or specifying your marketing preferences, you may:

- Visit www.codexinsurance.com/privacy;
- Speak to us directly by phoning us on +61 2 8044 1439; or
- Email us at info@codexinsurance.com.

CONTACT DETAILS

Address: Level 32, 200 George Street, Sydney, NSW, 2000

Website: www.codexinsurance.com

Phone: +61 2 8044 1439

Email: info@codexinsurance.com