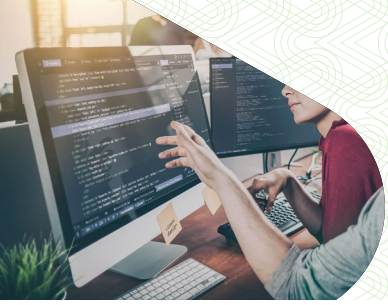

Cyber Liability Insurance

Proposal form

IMPORTANT NOTICES TO THE APPLICANT

COMPLETING THIS PROPOSAL FORM

This proposal forms the basis of any insurance contract entered. Please complete it fully and carefully, remembering to sign the declaration. If you have insufficient space to complete any of your answers, please attach a signed and dated addendum. Any documents attached to the proposal will form part of the proposal. If you have any doubt over the questions or completing this proposal, please contact your insurance agent, as any non-disclosure may affect your right of recovery under this policy.

CLAIMS MADE COVER

Cyber Insurance is issued on a 'Claims Made' basis. It only provides cover if a claim is made against you, by some other person during the period when the policy is in force.

It does not provide cover if a claim arises out of circumstances committed, attempted, or alleged to have been committed or attempted before the retroactive date stipulated in the schedule in the policy.

Section 40(3) of the Insurance Contracts Act 1984 (Cth) applies to this type of policy. That sub-section provides that if you become aware, during the period when the policy is in force, of any facts which might give rise to a claim against you by some other person, then provided that you notify the insurer in writing of the matter as soon as was reasonably practicable after you became aware of those facts but before the insurance cover provided by the policy expires, the insurer may not refuse to indemnify merely because a claim resulting from the matter is not made against you while the policy is in force.

If you, inadvertently or otherwise, do not notify the relevant occurrence or facts to the insurer before the expiry of the policy, you will not have the benefit of section 40(3) and the insurer may refuse to pay any subsequent claim, notwithstanding that the facts or events giving rise to it or the circumstances alleged in it may have taken place during the policy period.

If a claim is made against you by some other person during the policy period but is not notified to the insurer until after the policy has expired, the insurer may refuse to pay or may reduce its payment under the policy if it has suffered any financial prejudice as a result of the late notification.

DUTY OF DISCLOSURE

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

You have this duty until the insurer agrees to insure you. You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell the insurer anything that:

- reduces the risk the insurer insures you for; or
- is common knowledge; or
- the insurer knows or should know as an insurer; or
- the insurer waives your duty to tell the insurer about.

IF YOU DO NOT TELL THE INSURER SOMETHING

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

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

SUBROGATION AGREEMENT

If another person or company is liable to compensate you or hold you harmless for part or all of any loss or damage otherwise covered by our policy, but you agree with that person or company (either before or after the inception of our policy) that you would not seek to recover any loss or damage from them, we will not cover you for this loss or damage.

PRIVACY STATEMENT

Delta Insurance Australia Pty Ltd is committed to protecting your privacy. We have adopted the Australian Privacy Principles (**APPs**) contained in the Privacy Act 1988 (Cth) (**Privacy Act**). The APPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information.

Any Personal Information we collect about you will only be used for the purposes indicated in our Privacy Policy and only in the instance you have provided us with your consent or as otherwise required by law.

We will need to collect personal information from you or your insurance agent to assist with assessing your risk so that we can offer our products and services.

USE OF YOUR INFORMATION

The information collected will be used for the purpose in assisting us with underwriting and administrating your insurance cover on behalf of the Insurers we represent. Where reasonable and practicable to do so, we will collect your Personal Information only from you. To verify your identity, we may obtain or verify your Personal Information from a third party.

Information collected can also be used towards improving our customer service, product data research analysis and to advise you of any other products and services that may be of interest to you.

SECURITY OF YOUR INFORMATION

Your Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification, or disclosure.

When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your Personal Information. However, most of the Personal Information is or will be stored in client files which will be kept by us for a minimum of 7 years.

Whilst underwriting and reviewing your policy, we may share your information with your insurance agent, claims assessors, and to third party administrators providing related services to your insurance policy. Your information will be provided to the Insurer's we represent, based in the UK and whose details we will provide to you when issuing an insurance quotation.

By providing us with your Personal Information, you consent to us disclosing your information to such entities without obtaining your consent on a case-by-case basis.

FURTHER INFORMATION

We understand that you may not want to share with us the information which is requested to review your insurance policy, and this may affect our ability in providing and assessing an insurance policy.

For more information regarding how we collect, store, use and disclose your information, please read our privacy policy located at www.deltainsurance.com.au or alternatively you can contact us at contactus@deltainsurance.com.au.

Delta Insurance Australia Pty Ltd (ABN 83 652 033 933) is an Authorised Corporate Representative (CAR 001296353 of DIA Licence Pty Ltd (ACN 654 160 513) afsl 535427.

APPLICANT DETAILS

1 Name of Applicant (including Subsidiaries to be insured):

2 ABN:

3 Principal Address:

4 Year Established:

5 Website Address:

6 Please advise the number of staff (including Directors and Principals): Australia Overseas

7 During the past five years have any of the entities changed their names, or has there been any other business purchased e.g., merger or consolidation taken place? ○ Yes ○ No

8 Please outline the nature of the Applicant's business including a full description of the Applicant's activities:

FINANCIAL INFORMATION

9 Please provide the following turnover split:

Country	Last Financial Year AUD (actual)	Current Financial Year AUD (projected)
Australia	$	$
New Zealand	$	$
Asia	$	$
UK & Europe	$	$
USA & Canada	$	$
Rest of the World	$	$
Total	$ 0	$ 0

DATA INFORMATION

10 What types of Personal information does the Applicant collect, process & store?

○ Credit Card Information (please complete Q.11)
○ Customer Personal Details
○ Health Care Information
○ Third Party Intellectual Property or Trade Secrets
○ Banking and Financial Account Information
○ Personal Identity (e.g. drivers license)

11 When Credit Card information is stored, is the Applicant required to comply with payment card industry standards? ○ Yes ○ No

If yes, please select industry standard level:

○ Level 1 ○ Level 2 ○ Level 3 ○ Level 4 ○ Outsourced to Third Party Provider

12 Please estimate the total number of individual records held by the Applicant including number of customer records and credit card transactions:

○ 0 - 1,000 ○ 1,001 – 10,000 ○ 10,001 – 20,000 ○ 20,001 – 50,000
○ 75,001 – 100,000 ○ 100,0001 – 200,000 ○ 200,001 – 500,000 ○ Other (specify)

13 What percentage of the Applicant's income is derived from e-commerce activities?

○ None ○ 0 – 5 % ○ 6 – 15% ○ 16 – 25% ○ 26 – 50% ○ 50 -100%

PRIVACY INFORMATION

14 Does the Applicant have a Privacy Policy in place? ○ Yes ○ No

If yes:

(a) When was it last reviewed for updates?

(b) Are staff provided with a copy of this policy or advised where they can contain a copy (eg. Such as your website or at reception)? ○ Yes ○ No

(c) If required, does it comply with the Australian Privacy Principals? ○ Yes ○ No

If no to having a privacy policy in place, please provide details regarding data protection procedures of the Applicant:

15 Does the Applicant have a key person formally appointed as responsible for overall privacy management? ○ Yes ○ No

COMPUTER NETWORK & DATA RECOVERY:

16 Does the Applicant uses multifactor authentication (MFA) for cloud-based services (such as cloud-based email account, internet banking and accounting software) and for all remote access to the network? ○ Yes ○ No

17 Does the Applicant allow remote access into their environment without a Virtual Private Network (this requirement is not relevant for any cloud-based services)? ○ Yes ○ No

18 Does the Applicant provide regular (at least annually) cyber security awareness training, including anti phishing to all individuals who have access to the Insured's Organisation network or confidential / personal data? ○ Yes ○ No

19 Does the Applicant regularly back-up critical / important data to an offline location (disconnected from the live environment) and ensure that these backups can be restored? ○ Yes ○ No

20 With regards to maintaining regular backup and recovery procedures for all critical, data and information assets; how often is data backed up to a:

(a) Local server: ○ Daily ○ Weekly ○ Monthly ○ Other (specify):

(b) Cloud hosted data centre disconnected from the live environment:

○ Daily ○ Weekly ○ Monthly ○ Other (specify):

21 Does the Applicant have procedures in place to identify malicious emails or links? (Such as IT security/social engineering fraud risk policy or annual staff cyber training) ○ Yes ○ No

22 Does the Applicant have network and security monitoring controls in place to detect breaches of data security? ○ Yes ○ No

If yes, are critical alerts escalated immediately? ○ Yes ○ No

23 Does the Applicant, including via their IT consultants, have up-to date antivirus, firewalls and software security protection for:

(a) All external network connection points? ○ Yes ○ No

(b) Internally within the network to protect sensitive resources? ○ Yes ○ No

(c) All mobile equipment e.g. Laptops, Mobile Phones etc? ○ Yes ○ No

24 Is critical and sensitive data encrypted at the following stages?

(a) At rest? ○ Yes ○ No

(b) In transit? ○ Yes ○ No

(c) On portable media (laptops)? ○ Yes ○ No

25 Does the Applicant introduce password procedures to assist with the mitigation of a security breach, such as:

(a) Passwords to be changed on a regular basis e.g. Every 72 Days? ○ Yes ○ No

(b) Impose Strong Password Discipline e.g., Uppercase, Lowercase and Symbols? ○ Yes ○ No

26 How quickly can the Applicant restore critical systems following a network interruption:

○ < 6 Hours ○ 6 – 12 hours ○ 12 – 24 hours ○ > 24 hours

27 Where does the Applicant store critical & sensitive information:

(a) In an offsite secure location? ☐ Yes ☐ No

(b) Own Premises? ☐ Yes ☐ No

(c) Outsourced through a cloud hosting provider? ☐ Yes ☐ No

28 Are all physical records securely destroyed? ☐ Yes ☐ No

OUTSOURCING MANAGEMENT

29 For any third-party provider that has access to critical or private information:

(a) Does the Applicant have written agreements with IT consultants with regards to privacy/confidentiality clauses which requires them to comply with the privacy act? ☐ Yes ☐ No

(b) Please confirm what services are outsourced:

Type of Service	Yes/No	Name of Vendor
Cloud services	☐ Yes ☐ No	
Infrastructure/Server Management	☐ Yes ☐ No	
Managed Services (Backup and Hosting)	☐ Yes ☐ No	
IT Security	☐ Yes ☐ No	
Business Critical Software Services	☐ Yes ☐ No	
Payment Processing	☐ Yes ☐ No	
Point of Sale	☐ Yes ☐ No	

INCIDENT INFORMATION

30 Does the Applicant have a data breach response plan in place in the event of a security breach or system failure? ☐ Yes ☐ No

If yes, how often are these plans reviewed?

MEDIA LIABILITY

31 Does the Applicant have a process to review all content prior to posting on the Applicant's Internet Site? ☐ Yes ☐ No

If yes, is the review performed by qualified legal counsel? ☐ Yes ☐ No

Does the review include screening the content for the following:

(a) disparagement issues? ☐ Yes ☐ No

(b) copyrighting infringement? ☐ Yes ☐ No

(c) trademark infringement? ☐ Yes ☐ No

(d) invasion of privacy? ☐ Yes ☐ No

If the Applicant does not have a process to review all content prior to posting, please describe procedures to avoid the posting of improper or infringing content:

FRAUD CONTROLS

32 Is there a social engineering fraud risk management strategy in place? ☐ Yes ☐ No

33 Does the Applicant verify new customer or supplier bank account information (including Name, Address and bank account details) prior to initiating any financial transaction with such supplier or customer? ☐ Yes ☐ No

34 Does the Applicant have a call-back procedure to pre-agreed contact phone numbers, with customers or suppliers to:

(a) Authenticate any fund transfer instructions greater than $25,000 prior to transfer? ☐ Yes ☐ No

(b) Verify email change requested to supplier or customer bank account details (including account number, email address, contact information, bank routing number)? ☐ Yes ☐ No

35 Do all fund transfers greater than $10,000 require at least two members of staff to authorise or a supervisor/manager to sign-off? ○ Yes ○ No

STAMP DUTY

36 Please provide the approximate percentage of revenue / turnover applicable to each state or territory:

NSW	VIC	QLD	SA	NT	WA	ACT	TAS	O/S	Total
									0

COVER REQUIRED

37 Please select cover limit & retention required:

Coverage Limit	○ $250,000	○ $500,000	○ $1,000,000	○ $2,000,000	○ $5,000,000
Retention	○ $1,000	○ $2,500	○ $5,000	○ $10,000	○ $20,000

INSURANCE HISTORY

38 Has the Applicant ever had any insurance declined or cancelled, renewal refused, special conditions imposed, or a claim rejected? ○ Yes ○ No

If yes, please provide details:

39 Can you please provide details of the Applicant's current cyber insurance cover:

Current insurer: Expiry Date:

Limit of indemnity: $ Retention: $ Retroactive date:

CLAIMS HISTORY

40 Have any losses, claims, circumstance, cyber events or privacy breaches been made or brought against the Applicant or any of its directors, officers, or employees in the last five years (whether insured or not)? ○ Yes ○ No

41 Have the Applicant or any of its directors, officers, or employees been the subject to any regulatory, administrative or governmental investigation in the last five years (where insured or not)? ○ Yes ○ No

42 Have any crime losses or social engineering incidents been sustained by the Applicant in the last five years? ○ Yes ○ No

43 Is the Applicant, after enquiry, aware of any act, error, omission, event, circumstance, or incident which may give rise to a claim, proceeding or demand, or any regulatory, administrative or governmental investigation or crime loss? ○ Yes ○ No

If Yes to any of the above, please provide details as well as a copy of your claims history where applicable:

DECLARATION

I as the authorised undersigned partner, principal, or director, after full enquiry declare as follows:

(a) I am authorised by all Applicants to make this proposal.

(b) I have read and understood the duty of disclosure, located at the front of this proposal form.

(c) I have read and understood this proposal and any accompanying documentation, and acknowledge the contents herein are true and accurate.

(d) I understand that, up until a contract of insurance is entered into, I am under an ongoing obligation to immediately inform Delta Insurance Australia of any change in the facts or statements contained in this proposal form or in the accompanying documentation.

(e) I understand that should information provided be misleading or fraudulent, the contract may be voided in its entirety as per the Insurance Contracts Act 1984.

I agree although the signing of this proposal does not bind the underwriter to effect insurance, I acknowledge that the particulars and statements contained in this proposal and in the accompanying documentations shall be the basis of the insurance contract should a policy be effected; and further, I acknowledge that the proposal and the accompanying documentation will be incorporated in such policy.

Full Name: Title:

Signature: Date:

RESET FORM SAVE AS PDF