Cyber Liability
(long form)

Proposal form

NOTICE

This is a proposal form for a claims made policy. The policy will only respond to claims and/or circumstances which are first made against you and notified to Delta Insurance New Zealand Limited during the policy period.

This proposal forms the basis of any insurance contract entered into. Please complete it fully and carefully, remembering to sign the Declaration. If you have insufficient space to complete any of your answers please continue on a separate attachment.

You have an ongoing duty to disclose all material facts and failure to do so could prejudice future claims.

COMPANY INFORMATION

1 Name of Insured:

2 Primary address

3 Number of office locations in New Zealand:

Please note any subsidiaries including any international locations:

Please provide details on the interconnectivity of IT systems between office locations:

4 Web site:

BUSINESS ACTIVITIES

5 Business description:

6 Company details:

Country	Gross revenue last financial year	Estimated gross revenue this financial year	Number of staff	Number of staff with access to IT systems	Approximate number of third party/client records stored
NZ	$	$			
Australia	$	$			
USA	$	$			
UK	$	$			
Europe	$	$			
Asia and Pacific Islands	$	$			
Other*	$	$			

* Please specify other countries:

7 What proportion of the company's gross revenue is derived from e-commerce? %

8 What percentage of third party / client information stored consists of the following:

Type of information	Percentage
Business and customer information	%
Credit card information	%
Bank account details	%
Financial account information	%
IRD / Tax File Numbers / Social Security Numbers	%
Intellectual property	%
Trade secrets	%
Medical records or healthcare information	%
Total (should equal 100%)	0 **%**

9 If credit card is selected above does the company comply with PCI standards?

○ Level 1 ○ Level 2 ○ Level 3 ○ Level 4 ○ Non-compliant ○ or name third party provider:

10 Does the company share sensitive information with third party contractors, suppliers or customers? ○ Yes ○ No

If Yes, (a) Are they provided with access to your system? ○ Yes ○ No

(b) Are access rights restricted? ○ Yes ○ No

(c) Are access rights removed within 48 hours after the completion of contracts? ○ Yes ○ No

11 Does the company transfer sensitive information across international borders? ○ Yes ○ No

12 Does the company abide by local data privacy regulations e.g. General Data Protection Regulation (GDPR) (EU), Privacy Amendment (Notifiable Data Breaches) Act 2017 (Australia), Privacy Act 2020 (New Zealand) or any equivalent? ○ Yes ○ No

13 Does the company use Industrial Control Systems (ICS)? ○ Yes ○ No

(a) Supervisory Control And Data Acquisition (SCADA) ○ Yes ○ No

(b) Distributed Control Systems (DCS) ○ Yes ○ No

(c) Programmable Logic Controllers (PLCs) ○ Yes ○ No

DATA PROTECTION PROCEDURES

14 Does the company have the following written policies:

(a) Data protection policy ○ Yes ○ No

(b) Privacy policy ○ Yes ○ No

(c) Confidentiality policy ○ Yes ○ No

15 Are the above policies distributed to employees? ○ Yes ○ No

16 Do all employees including senior management undergo cyber security training at least annually? ○ Yes ○ No

17 Does the company perform background checks on all employees and independent consultants? ○ Yes ○ No

18 Does the company have physical security controls in place to prohibit and detect unauthorised access to their computer system and data centre? ○ Yes ○ No

19 Does the company allow employees to Bring their Own Device? ○ Yes ○ No

If Yes, what controls are in place for network access and use?

20 Please confirm MFA is required and enabled for all remote access, for all employees and/or contractors, for all internet facing parts of your business? ○ Yes ○ No

21 Is MFA enabled on any customer accessed portal and/or services? ○ N/A ○ Yes ○ No

22 Please note below remote access points to your business which don't have MFA in place and what alternative method is used to secure remote access?

23 What steps do you take to verify, enforce and audit the use of MFA for all users, for all internet access points to your business including all cloud resources used by your business?

24 Please confirm MFA is required and enabled for remote access to all company email accounts? ○ Yes ○ No

25 Please confirm MFA is required and enabled to access all cloud resources used by your business? ○ Yes ○ No

26 Does the company implement antivirus protection systems on all computers and devices? ○ Yes ○ No

27 Does the company implement firewalls on computers and devices? ○ Yes ○ No

28 Does the company implement intrusion detection and prevention systems? ○ Yes ○ No

29 Does the company use endpoint protection and monitoring solutions on its network, on all end-points? ○ Yes ○ No

If Yes, please specify which product:

30 Does the company monitor its network and computer systems for Breaches of Data Security, suspicious connections, or malicious IP addresses? ○ Yes ○ No

If Yes, please detail how this is carried out (for example SIEM Tools, External Security Operations Centre (SOC) etc.):

31 Has the Company conducted any of the following in the last 12 months:

(a) Cyber Security Assessment? ○ Yes ○ No

(b) Penetration Test? ○ Yes ○ No

(c) Internet Perimeter Scan? ○ Yes ○ No

If Yes, was it conducted by an external vendor? ○ Yes ○ No

If Yes, please attach the summary of the findings, recommendations, and status of the implementation of the action plan to address the recommendations made in the assessment or scan.

32 Does the company implement Distributed Denial Of Service protection? ○ Yes ○ No

33 Is application whitelisting implemented on all systems and devices? ○ Yes ○ No

34 Are the latest updates and security patches applied within a month of release? ○ Yes ○ No

35 Does the company use any end-of-life or unsupported software/platform/products among all IT and Operational Technology (OT) systems? ○ Yes ○ No

If Yes, is it segregated from the rest of the network and not connected to the internet? ○ Yes ○ No

DATA BACKUP & SYSTEMS RECOVERY

36 Does the company have and maintain backup and recovery procedures for all:

(a) Mission and Critical Systems? ○ Yes ○ No

(b) Data and information assets? ○ Yes ○ No

If Yes, are they encrypted? ○ Yes ○ No

37 Does the company perform regular system/ file backups? ○ Yes ○ No

38 Do they cover the company's critical data? ○ Yes ○ No

39 Are backups stored: ○ Offsite? ○ On premise?

(a) If On Premise, are they:

(i) Connected to your network (e.g. NAS)? ○ Yes ○ No

(ii) Or physically separated (e.g. USB, CD)? ○ Yes ○ No

(iii) Are credentials stored locally? ○ Yes ○ No

(b) If stored in Cloud:

(i) Is Multi-Factor Authentication enforced? ○ Yes ○ No

(ii) Are credentials stored locally? ○ Yes ○ No

40 Has your organisation tested system/file backups in the last six months? ○ Yes ○ No

If Yes, were systems/files restored successfully? ○ Yes ○ No

41 Do accounts with the ability to create, modify or delete backups follow password complexity and rotation requirements? ○ Yes ○ No

If Yes, is MFA also enforced? ○ Yes ○ No

42 Does the company implement the following:

		Frequency updated	Date of last backup audit/test
Business Continuity Plan (BCP)	○ Yes ○ No	○ Daily ○ Monthly ○ Yearly	
Disaster Recovery Plan (DRP)	○ Yes ○ No	○ Daily ○ Monthly ○ Yearly	

43 In your BCP / DRP, how long would it take to be fully operational after an incident?

44 If your IT network failed, which of the following would best describe the impact to your company (please tick):

○ Minimal impact, operations can continue as usual.
○ Delayed impact to revenue and operations.
○ Immediate impact to revenue and operations.
○ Entire interruption to revenue and operations.

45 Please describe your network contingency / redundancy / resilience in place to mitigate system interruptions or failures.

OUTSOURCED SERVICES

46 Identify if the company uses vendors for the following services:

Cloud/Backup	○ Yes	○ No	Vendor:
Hosting	○ Yes	○ No	Vendor:
Internet service provider	○ Yes	○ No	Vendor:
Business critical software	○ Yes	○ No	Vendor:
Payment processing	○ Yes	○ No	Vendor:
Point of sale hardware provider	○ Yes	○ No	Vendor:
Cyber security services	○ Yes	○ No	Vendor:
Managed security services	○ Yes	○ No	Vendor:

47 Is co-operation and support provided by outsourcers in the event of a data breach? ○ Yes ○ No

INCIDENT INFORMATION

48 Has the Company been the subject to an investigation or audit in relation to data protection, a Data Subject Access Request or an Enforcement Notice by any Data Protection Authority or other regulator? ○ Yes ○ No

If Yes, please provide full details:

49 During the past three (3) years, has the Insured experienced any occurrences, Claims or losses related to the Insured's system failure or failure of the Cloud or does the Insured have knowledge of a situation or circumstance which might otherwise result in a Claim against the Insured with regard to issues related to the insurance sought? ○ Yes ○ No

If Yes, please provide full details:

INSURANCE HISTORY

50 Have you had any similar insurance during the past three years? ○ Yes ○ No

51 Please provide details of your current Cyber insurance policy:

Insurer Expiry date

Limit Excess Premium

52 In the past three years, has the Insured been declined any similar cyber insurance policy, or has any insurer cancelled any previous cyber insurance policy? ○ Yes ○ No

If Yes, please provide a detailed description of the circumstance.

53 Have any claims been made against the Insured or any of its former or current directors, officers, employees, subsidiaries or independent contractors with regard to the coverage sought in the past three years? ○ Yes ○ No

If Yes, please provide a detailed description of the circumstance.

54 Is the Insured or any of its former or current directors, officers, employees, subsidiaries or independent contractors aware of any acts, errors, omissions or other circumstances, which may reasonably result in a claim relative to the insurance sought? ○ Yes ○ No

If Yes, please provide a detailed description of the circumstance.

DECLARATION

On behalf of all proposed Applicants I/We declare and agree that all information provided in this proposal or attachments is true and correct in every respect and that all information that may be material in considering this proposal form has been fully and accurately disclosed to Delta Insurance New Zealand Limited in writing in a manner which would not mislead a prudent insurer.

I/We agree that this declaration shall be the basis of and incorporated in the insurance contract and that the insurance contract may be avoided (amongst other things) if any statement in this proposal is "substantially incorrect" or "material" as both terms are defined in the Insurance Law Reform Act 1977.

I/We undertake to inform Delta Insurance New Zealand Limited of any material alteration to the above information whether occurring before or after the completion of this insurance contract.

I/We understand that:

(a) I/We am/are obliged to advise Delta Insurance New Zealand Limited of any information which may be material to its consideration of this application. This information includes all information I/We know (or could reasonably be expected to know) which could influence the judgement of Delta Insurance New Zealand Limited whether or not to accept this application and (if accepted) on what terms, including cost and otherwise.

(b) Failure to provide this information may result in Delta Insurance New Zealand Limited refusing to provide the insurance.

(c) I/We have certain rights of access to and correction of this information.

Full name & title of individual:

Signature of Policyholder: Date:

RESET FORM SAVE AS PDF

Lloyd's is a member of the Insurance Council of NZ and we adhere to the Fair Insurance Code, which provides you with assurance that we have high standards of service for our customers.