

Delta Insurance New Zealand Ltd. Level 8, 57 Fort Street, Auckland 1010. PO Box 106 276, Auckland 1143. Tel 09 300 3079 [deltainsurance.co.nz](http://deltainsurance.co.nz)

## Cyber Insurance (long 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	\$	\$			
Africa	\$	\$			
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	%
<b>Total</b>	<b>100 %</b>

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**, Are they provided with access to your system?  Yes  No  
     Are access rights restricted?  Yes  No  
     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) or any equivalent?  Yes  No
- 13 Does the company use Industrial Control Systems (ICS)?  Yes  No  
 Supervisory Control And Data Acquisition (SCADA)  Yes  No  
 Distributed Control Systems (DCS)  Yes  No  
 Programmable Logic Controllers (PLCs)  Yes  No

**Data Protection Procedures**

- 14 Does the company have the following written policies:  Yes  No  
 Data protection policy  Yes  No  
 Privacy policy  Yes  No  
 Confidentiality policy  Yes  No
- 15 Are the above policies distributed to employees?  Yes  No
- 16 Are there restrictions on staff’s ability to download and install software?  Yes  No
- 17 Is application whitelisting implemented on all systems and devices?  Yes  No
- 18 Are user’s activities monitored?  Yes  No
- 19 Do all employees including senior management undergo cyber security training at least annually?  Yes  No
- 20 Are employee system access rights restricted?  Yes  No  
 Are employee access rights audited at least annually?  Yes  No  
 Are access rights removed within 48 hours after the termination of employees?  Yes  No
- 21 Does the company perform background checks on all employees?  Yes  No

22 Please provide the number of:

Country	Computers	Servers	Portable devices (mobile phones, tablets)	Other (specify)
NZ				
Australia				
USA				
UK				
Europe				
Asia				
Africa				
Other*				

\* Please specify other countries:

23 Are physical controls in place to prevent access to data centres?  Yes  No

24 Are passwords implemented to access network connected devices?  Yes  No

25 Explain the policies in place around changing passwords and password requirements:

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

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

27 Is Wi-Fi connectivity protected?  Yes  No

28 Is authentication in place for remote user connections to the company network?  Yes  No

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

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

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

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

33 Are the latest updates and security patches applied automatically or within the month of release?  Yes  No

**Data Backup & Systems Recovery**

34		Frequency of backups	Date of last backup audit/test	Frequency of backup audit/test
	Mission Control systems	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Daily <input type="radio"/> Monthly <input type="radio"/> Yearly		<input type="radio"/> Daily <input type="radio"/> Monthly <input type="radio"/> Yearly
	Data and information assets	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Daily <input type="radio"/> Monthly <input type="radio"/> Yearly		<input type="radio"/> Daily <input type="radio"/> Monthly <input type="radio"/> Yearly

35 Does the company implement encryption on data assets?  Yes  No

36 Does the company implement the following:

	Frequency updated	Date of last backup audit/test
Business Continuity Plan (BCP)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Daily <input type="radio"/> Monthly <input type="radio"/> Yearly	
Disaster Recovery Plan (DRP)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Daily <input type="radio"/> Monthly <input type="radio"/> Yearly	

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

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

38 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

**Outsourced Services**

39 What is the size of your annual IT budget: \$ \_\_\_\_\_ Approximate proportion spent on IT security: %

40 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: \_\_\_\_\_
- Managed security services  Yes  No Vendor: \_\_\_\_\_

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

**Incident Information**

42 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:

43 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:

44 Is there any other information in your possession material to an estimation of the risk to be insured and/or information of any nature which the underwriters should be made aware of?  Yes  No

If Yes, please provide full details:

**Insurance History**

45 Have you had any similar insurance carried during the past three years?  Yes  No

46 Please provide details of your current Cyber insurance policy:

Insurer		Expiry date
Limit	Excess	Premium

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

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

**47** 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.

**48** 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 Ltd 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 Ltd 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 Ltd 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 Ltd 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 Ltd refusing to provide the insurance.
- (c) I/We have certain rights of access to and correction of this information.

Signature of Principal, Partner or Director:

Full name of individual:

Date: