

# PROPOSAL FORM

## Cyber Insurance



### DUTY OF DISCLOSURE

This proposal form is to be completed by the Applicant or an Authorised Officer of the Applicant.

The information provided to Vero Liability in this proposal form will be the basis of any contract of insurance entered into.

You must disclose to Vero Liability Insurance Limited all information which is material to it in deciding whether to issue insurance cover to you, and if so on what terms and/or premium. This includes but is not limited to any circumstances or conduct which might lead to a claim being made against you. This may also include information which is additional to the questions that we have asked. The duty to disclose material information occurs prior to the commencement of cover, prior to each renewal or whenever the policy is varied. This means that prior to renewal or any policy variations, as well as advising of new information you also need to advise us of any alterations to the facts previously notified. Failing to disclose material information may result in your policy being avoided. This means that your policy would be deemed to have never existed and no claims would be payable.

If there is insufficient space to provide full information in this proposal, please attach additional sheets.

### WHEN IN DOUBT DISCLOSE.

### IMPORTANT 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 known to the Insured and notified to Vero Liability Insurance Limited during the policy period. The policy will not provide cover for:

- ◆ Events that occurred prior to the retroactive date of the policy (if specified).
- ◆ Claims made after the expiry of the policy period (or extended reporting period if available) even though the act giving rise to the claim may have occurred during the policy period.
- ◆ Claims notified or arising out of facts or circumstances notified under any previous policy or noted on the current proposal form or any previous proposal form.
- ◆ Claims made, threatened or intimated prior to the commencement of the policy period.
- ◆ Claims arising from circumstances known to the Insured at the commencement of the policy period as having the potential to give rise to a claim.

## A. Applicant Details

Name of applicant including trading names, names of subsidiaries and any other parties to be insured

Address

Website Address

Email Address

Contact Person

Phone Number

Mobile Number

Broker / Agent

Please specify details of your activities/businesses

### 1. Turnover/Revenue and General Information

Country	Gross Turnover/Revenue	Gross Turnover/Revenue created online (eg from e-commerce)
New Zealand	\$	\$
Australia	\$	\$
USA/Canada	\$	\$
Rest of the world	\$	\$

## 2. IT Budget & Security Spend

What is your IT budget?	\$
What percentage of your budget is allocated to IT security	\$

## 3. Quality and Quantity of Data, Online Activities & Services

What type of sensitive data is your Company maintaining/processing?

<input type="checkbox"/> Personally Identifiable Information (PII)	<input type="checkbox"/> Personal Health Information (PHI)
<input type="checkbox"/> Payment Card Information (PCI)	<input type="checkbox"/> Usernames and Passwords
<input type="checkbox"/> Intellectual Property (IP)	

Please state the (estimated) volume of sensitive data (number of unique records) your Company maintaining/processing

<input type="checkbox"/> < 1,000	<input type="checkbox"/> 1,000-10,000	<input type="checkbox"/> 10,000-100,000	<input type="checkbox"/> 100,000 +
----------------------------------	---------------------------------------	---	------------------------------------

Please state the (estimated) number of user endpoints (desktops, laptops, portable devices)

<input type="checkbox"/> < 25	<input type="checkbox"/> 26-50	<input type="checkbox"/> 51-100	<input type="checkbox"/> 100 +
-------------------------------	--------------------------------	---------------------------------	--------------------------------

## B. Cover Required

### 1. Requested Insurance

Coverage	Limit Required					
Limit of Indemnity	<input type="checkbox"/> \$250,000	<input type="checkbox"/> \$500,000	<input type="checkbox"/> \$1,000,000	<input type="checkbox"/> \$2,000,000	<input type="checkbox"/> \$5,000,000	<input type="checkbox"/> \$10,000,000
Business Interruption	<input type="checkbox"/> \$250,000	<input type="checkbox"/> \$500,000	<input type="checkbox"/> \$1,000,000	<input type="checkbox"/> \$2,000,000	<input type="checkbox"/> \$5,000,000	<input type="checkbox"/> \$10,000,000
Systems Damage	<input type="checkbox"/> \$250,000	<input type="checkbox"/> \$500,000	<input type="checkbox"/> \$1,000,000			
Cyber Crime	<input type="checkbox"/> \$100,000	<input type="checkbox"/> \$250,000				
Extortion	<input type="checkbox"/> \$250,000	<input type="checkbox"/> \$500,000	<input type="checkbox"/> \$1,000,000	<input type="checkbox"/> \$2,000,000	<input type="checkbox"/> \$5,000,000	<input type="checkbox"/> \$10,000,000

### 2. Optional Extensions

- Named Cloud Service Provider Yes  No   
If yes please name Cloud Provider
- Fraudulent Impersonation Yes  No

### 3. Prior Insurance

- Do you currently hold, or have you ever held cyber insurance providing the same or similar coverage as the insurance sought? Yes  No
- Has any insurer ever cancelled or non-renewed a policy that provided the same or similar coverage as the insurance being applied for? Yes  No

## C. Third Party Services

- Do you outsource any part of your network, computer system or information security functions? Yes  No

2. If yes please give details

Function	Provider
<input type="checkbox"/> Management of entire IT system	
<input type="checkbox"/> Data Processing)	
<input type="checkbox"/> Application of Service Provider	
<input type="checkbox"/> Offsite Backup and Storage	
<input type="checkbox"/> Other Cloud Computing Services	

- Do you have a written and signed contract with the respective service provider(s) including a non-disclosure / confidentiality agreement? (N/A only if you do not outsource any part of your network, computer system or information security functions) Yes  No   
N/A

## D. IT Security

<b>1. Organisational Protection</b>		
a) Do you have a dedicated IT Security person or team who regularly reports to senior management?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
b) Are you required to be PCI compliant?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
c) Do you provide regular training to increase your staff's security awareness and to prepare employees to be more resilient and vigilant against phishing?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
d) Do you have a password policy and is it enforced e.g. by complexity (strong passwords) and rotation (regular change)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
e) How often are passwords required to be changed?		
f) Do you regularly – at least monthly – patch (update) your systems and applications?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
g) Do you immediately apply critical patches (updates) to your systems and applications?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
h) Do you have an incident response plan and is it at least annually tested?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
i) Do you have a disaster recovery plan and is it at least annually tested?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
j) Do you restrict user access/privileges to a need-to-do-business only?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
k) Do you immediately remove access of terminated or temporary staff?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
l) Do you provide users remote access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
i. If yes, is access granted via a VPN or equivalent? and	Yes <input type="checkbox"/>	No <input type="checkbox"/>
ii. Does access require two-factor authentication (ie not just username and password)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
m) Do you have an information classification scheme (ie identify mission critical information assets)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
i. If yes, does the scheme take into account information confidentiality, integrity and availability?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<b>2. Technical Protection</b>		
a) Do you use anti-virus, anti-spyware or equivalent malware protection?		
i. If yes, are all malware protection software automatically updated?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
b) Are all internet access points to your network secured by firewall(s)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
c) Is it ensured that all default passwords on all computer systems (e.g. router) are changed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
d) Is all personally identifiable and confidential information encrypted when:		
i. At rest?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
ii. In transit/motion?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
e) Do you perform regular, automatic off-site backups?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
i. If yes, how often?	At least daily <input type="checkbox"/>	At least weekly <input type="checkbox"/>
f) Do you test retrieval of backups?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
g) Do you have a business continuity plan and is it at least annually tested?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
h) Do you run vulnerability scans or undertake penetration testing against your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

## E. Prior Insurance

Has any insurer in respect of the risks to which this proposal relates ever:		
1. declined a proposal, refused renewal or terminated any insurance?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2. required an increased premium or imposed special conditions?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
3. declined an insurance claim by the Applicant or reduced its liability to pay an insurance claim in full (other than by application of an Excess)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If Yes to any of the above please give details		

## F. Security Events and Loss History

Within the last 3 years, have you suffered a violation of IT Security, network damage, system corruption or loss of data?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes, please provide details and advise what was the financial loss associated with it for your company?		
Within the last 3 years have you notified your customers that their information was or could be compromised	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Within the 3 years has a customer claimed that their personal data has been compromised?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes, what was the financial loss associated with it for your company?		

## G. Past Claims

Has any claim been made against the Applicant or any principal or director (including principal or director of any previous business) consultant or employee in respect of the risks to which this proposal relates?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Has the Applicant or any principal, partner, director, consultant or employee incurred any other loss or expense which might be within the terms of this insurance	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If Yes, please give details		

## H. Potential Claims

Is any principal, director, partner consultant or employee, after enquiry, aware of any circumstances which might:		
1. give rise to a claim against the Applicant or his/her predecessors in business or any present or former principals, partners, directors, consultants or employees?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2. result in the Applicant or his/her predecessors in business or any present or former principals, partners, directors, consultants or employees incurring any losses or expenses which might be within the terms of this insurance cover (this includes but not limited to disciplinary hearings)	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If Yes, please give details		

## I. Declaration

On behalf of all proposed Insureds, I/We declare and agree that:

- the information and answers given in this proposal are in every respect true and correct and that Vero Liability has been made aware of all information that may be material in considering this proposal.
- this proposal and declaration shall be the basis of and incorporated in the insurance contract.
- I/We warrant that we will notify Vero Liability of any material alteration to these facts whether occurring before or after the completion of this insurance contract.
- Vero Liability is authorised to give to or obtain from any other insurers or any insurance broker or other party any information relating to this insurance or any other insurance held by me/us or any claim made by me/us.

I/We understand that:

- Vero Liability is collecting the information on this proposal for the purpose of conducting its business, evaluating our insurance requirements and deciding whether to issue insurance cover and if so on what terms.
- failure to provide any of this information may result in Vero Liability refusing to provide the insurance.
- this information will be held by Vero Liability at 23-29 Albert Street, Auckland.
- I/We have certain rights of access to and correction of this information.

**Signed:**

**Title:**

**Date:**

**If this proposal form is being completed electronically, please print the completed form to sign.**

**Note: Completion of this proposal does not bind the Applicant or Vero Liability to enter into a contract of insurance.**

**Vero Liability Insurance Limited**  
Level 32, ANZ Centre, 23-29 Albert Street  
Private Bag 92055 Auckland New Zealand  
Telephone 09 306 0350

[www.veroliability.co.nz](http://www.veroliability.co.nz)