Proposal Form Cyber Liability

vero liability insurance limited

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.

1. General Information

1.1 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	

1.2 Business Activities

Please specify details of your activities/businesses

1.3 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	Number of third party/customer records held
New Zealand	$	$			
Australia	$	$			
USA/Canada	$	$			
Rest of the world	$	$			
Total	$0	$ 0	0	0	0

1.4 Type of Data

Type of Data	Percentage
Personally Identifiable Information (PII)	%
Personal Health Information (PHI)	%
Payment Card Information (PCI)	%
Intellectual Property (IP)	%
Total	100%

If payment card information is noted above does the company comply with PCI standards?

☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4

☐ Non-Compliant ☐ or name third party Provider

1.5 Requested Cyber Limit

Limit of Indemnity ☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐ $2,000,000 ☐ $5,000,000 ☐ $10,000,000

1.6 Third Party Services

Do you outsource any part of the following services to third party vendors:

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	Yes ☐	No ☐	Vendor:
Cyber Security Services	Yes ☐	No ☐	Vendor:
Managed Security Services	Yes ☐	No ☐	Vendor:

2. Previous Insurance Information

2.1 Prior Cyber Insurance

a)	Does the Applicant currently hold or ever held cyber insurance?	Yes ☐	No ☐
b)	Has any insurer declined a proposal, refused renewal or terminated any insurance?	Yes ☐	No ☐
c)	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 ☐	No ☐

2.2 Security Events and Loss History

Please answer the following questions by considering any time during the past three years.

a)	Have you had any **incidents, claims or suits** involving unauthorized access or misuse of your network, including embezzlement, fraud, theft of proprietary information, breach of personal information, theft or loss of laptops, denial of service, electronic vandalism or sabotage, computer virus or other incident?	Yes ☐	No ☐
b)	Have you experienced an **unplanned business interruption** of longer than four hours caused by a cyber incident?	Yes ☐	No ☐
c)	Have you experienced an **extortion attempt or demand** with respect to your computer systems?	Yes ☐	No ☐
d)	Have you received any **claims or complaints** with respect to allegations of defamation, invasion of privacy, theft of information, breach of information security, transmission of malware, participation in a denial of service attack, request to notify individuals due to an actual or suspected disclosure of personal information?	Yes ☐	No ☐

e)	Have you been subject to any **government action, investigation or subpoena** regarding any (alleged) violation of any privacy law or regulation?	Yes ☐	No ☐
f)	Are you aware of any **release, loss or disclosure of personally identifiable information** in your care, custody or control, or in the control of anyone holding such information on behalf of you?	Yes ☐	No ☐
g)	Are you aware of any **actual or alleged fact, circumstance, situation, error or omission, or potential issue** which might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for or any similar insurance presently or previously in effect or currently proposed?	Yes ☐	No ☐

If one question or more of this section 1.8 is answered with "Yes", please attach a description including complete details (cause, costs, notification, time to discover, recovery time and steps taken to mitigate future exposure) of each event (incident, claim etc.).

3. Identify

3.1 Cybersecurity Assessment

a)	Have you had an independent cybersecurity assessment in the last 12 months?	Yes ☐	No ☐
b)	If yes, were all recommendations made in the report implemented?	Yes ☐	No ☐
c)	Have you conducted a penetration test or external vulnerability scan in the last 12 months?	Yes ☐	No ☐
d)	Have you conducted a Business Impact Analysis (BIA) in the last 12 months?	Yes ☐	No ☐

Why an independent cybersecurity assessment? An independent cybersecurity assessment can provide a comprehensive analysis and review of an organisations security and privacy operations by detecting vulnerabilities and threats, displaying weak links, and high-risk practices. An assessment report can also include recommendations based on the findings of the assessment. This information provides us greater insights into your cybersecurity maturity posture and what you have or plan to undertake to improve it beyond information we can simply gather in a proposal form.

What is a penetration test? A cybersecurity assessment method wherein ethical hackers attempt to breach an organisation's security protocols, with permission, in order to identify vulnerabilities. It simulates a real-world attack to test a system's defences, providing valuable insights to improve security measures.

What is an external Vulnerability Scan? An automated process that scans a system, network, or application to identify potential security weaknesses, often known as vulnerabilities. Unlike a penetration test, it doesn't exploit these vulnerabilities but provides an inventory of potential points where an attack could occur.

What is a Business Impact Analysis (BIA)? A Business Impact Analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations from a cyber event. It forms a critical component for allocating appropriate security resources and business continuity planning.

3.2 Information Classification

a)	Do you have an information classification scheme to classify information with regards to confidentiality, integrity, and availability?	Yes ☐	No ☐

What is an Information Classification Scheme? A framework used by an organisation to categorise information based on its sensitivity and level of confidentiality. This helps in applying appropriate security controls to protect the data.

Why are we asking this question? IT security budgets are not limitless and no matter how secure you are, you are not immune to an attack. Therefore, it is important to identify your risk and allocate security resources based on the nature, criticality, and value of the information to ensure it is treated appropriately. Attributing criticality first requires an identification process.

3.3 Legacy Systems

a)	Do you use any software or hardware which has reached end-of-life or end-of-support status?	Yes ☐ ▶	No ☐
	▶ If yes, is it segregated from the rest of the network and not internet connected?	Yes ☐	No ☐

Why are we asking this question? Legacy software, hardware, and systems that are no longer supported by the vendor can be exposed to vulnerabilities where no patch (update) is available. This makes legacy systems vulnerable to cyber-attacks as they can be much easier for malicious actors to gain access. If you do have legacy systems, we want to understand the plans and controls that are in place to mitigate these risks.

3.4 Written Policies

a) Do you have any of the following written policies in place:			Date of last review:
Data Protection Policy	Yes ☐ ▶	No ☐	
Privacy Policy	Yes ☐ ▶	No ☐	
Confidentiality Policy	Yes ☐ ▶	No ☐	

4. Prevention and Detection

4.1 Software Updates / Patching

a) Within one month of release are all security and critical patches (updates) for your systems and applications deployed? Yes ☐ No ☐

What is Patching? The process of applying updates to software or a system, often to fix vulnerabilities or bugs that have been identified since the last release. Patches help enhance security, improve functionality, and maintain the stability of a system, making it an important part of regular system maintenance.

Why are we asking this question? A software update can be critical to patch a known software bug / security vulnerability that could inadvertently grant a malicious actor access to your systems. Not making it a requirement for all users to implement these updates or delaying the rollout for such updates opens a longer window for which a malicious actor can exploit such a security flaw.

Want to undertake more research on Patching? For more information on Patching see the advisory by CERT NZ here

4.2 User Access

a) Multi-factor Authentication (MFA)

Is Multi-Factor Authentication (MFA) enabled for?	• Office 365?	N/A ☐	Yes ☐	No ☐
	• Employees working from home / remote access?	N/A ☐	Yes ☐	No ☐
	• Systems containing sensitive third party information?	N/A ☐	Yes ☐	No ☐
	• Customer/Trade Account Login?	N/A ☐	Yes ☐	No ☐
	• Industrial Control Systems	N/A ☐	Yes ☐	No ☐

What is MFA? A user to internet-facing, administrative services, and other business critical systems is only granted access at such time as having presented two or more pieces of evidence for the purpose of authenticating and verifying that user is the right user.

Why are we asking this question? According to the CrowdStrike 2022 Global Threat Report 80% of attacks leveraged user identities. Tricking users into handing over their login credentials is a common tactic. MFA adds an additional layer of protection, making it harder for unauthorized users to gain access.

Want to undertake more research on MFA? For more information on MFA see the advisory by CERT NZ here

b) Do you restrict user access / privileges to a need-to-do-business basis only? Yes ☐ No ☐

Why are we asking this question? By restricting user access privileges to a need only basis the number of users that can access certain company resources and systems is reduced. This in turn reduces the number of accounts that if compromised by a malicious actor can access such critical resources and systems. Particularly important to restrict access for administrative permissions and sensitive information e.g. personal data.

c) Do you revoke all system access, accounts, and associated rights after termination of users (including employees, temporary employees, contractors, or vendors)? Yes ☐ No ☐

d) Do you restrict users from installing unauthorised software (implementation of application control) on their devices? Yes ☐ No ☐

What is application control? A security practice that restricts the applications that can be executed by users on a system. It helps to prevent harmful software or unauthorised applications from running, thereby protecting the system and data. This method is often implemented through a whitelist, where only approved software can operate, or a blacklist, where specific software is prevented from running.

Want to undertake more research on application control? For more information on application control see the advisory by CERT NZ here

e) Do you provide regular training to increase your staff's (including senior management and contractors) security awareness and to prepare employees to be more resilient and vigilant against phishing? Yes ☐ No ☐

What is phishing? Phishing is a type of social engineering where a malicious actor sends a fraudulent message in attempt to trick the recipient into revealing sensitive information (i.e. user name and password) or to deploy malicious software on the victim's system (i.e. by clicking a malicious link).

Why are we asking this question? Your staff are your first line of defence and often considered by malicious actors to be the weakest link in the chain. Providing staff frequent training can assist them to not fall victim to malicious emails, links and attachments and how to detect and report such suspicious activity. Furthermore, training can assist staff to act with good IT hygiene.

4.3 Default Credentials & Passwords

a) Do you ensure all default credentials and login details are frequently (ie, less than 60 or 90 days) changed upon set up? Yes ☐ No ☐

b) Do you have a password policy (ie, using long and complex password, enforce MFA based on criticality, etc) in place and is it enforced for all users including remote & privileged users? Yes ☐ No ☐

4.4 Securing Devices and Network

a)	Is there continually up-to-date malware protection in place on all web-proxies, email-gateways, workstations, laptops and any other applicable systems across your IT or Operational Technology (OT) infrastructure?	Yes ☐	No ☐
b)	Are all internet access points to your network secured by firewall(s)?	Yes ☐	No ☐
c)	Have you implemented network segregation?	Yes ☐	No ☐
d)	Do you monitor your network and identify security events?	Yes ☐	No ☐
e)	Are you utilising an Intrusion Detection System (IDS)?	Yes ☐	No ☐
f)	Are you utilising an Endpoint Detection and Response (EDR) solution?	Yes ☐	No ☐
g)	Is working from home / remote access only granted via a Virtual Private Network (VPN) or equivalent?	Yes ☐	No ☐
h)	Is all personally identifiable and confidential information encrypted when: i. At rest? ii. In transit/motion?	Yes ☐	No ☐

What is network segregation? Network segregation is partitioning a network into smaller parts and can be used to separate critical networks from the internet, as well as from other internal networks.

What is an Intrusion Detection System (IDS)? A device or software application that monitors a network or system for malicious activity or violations of policies. If such activities are detected, the IDS alerts the system administrator or, in more advanced systems, takes actions to block or minimise the impact of the threat.

What is an Endpoint Detection and Response (EDR)? A cybersecurity technology that continually monitors and collects data from endpoints, such as workstations and servers, to identify, investigate, and prevent potential cyber threats. EDR solutions provide enhanced visibility into endpoint activities, allow rapid response to incidents, and offer valuable insights to improve security strategies against future threats.

What is a Virtual Private Network (VPN)? A service that establishes an encrypted connection between a user's device and a network over the internet.

4.5 Industrial Control Systems (ICS) and Operating Technology

Only answer the following questions in 4.5 if you utilise Industrial Control Systems and / or Operation Technology otherwise skip to 4.6

What is an Industrial Control System (ICS)? The term Industrial control system (ICS) embraces several types of control systems and associated instrumentation used for industrial process control.

What is Operational Technology (OT)? Operational Technology (OT) is defined as collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process.

a)	Is OT segregated from the rest of the IT corporate network?	Yes ☐	No ☐
b)	Do you provide remote access to your industrial systems/networks	Yes ☐	No ☐
c)	Please describe your ability to maintain business operations in the event of downtime of your IT or OT network		
d)	Please highlight the redundancy processes that are in place to mitigate any operational technology / product line outage?		
e)	What patching controls are in place for the operational technology network?		

4.6 Verifying financial details

a)	Before initiating an email request from a supplier or customer to make a transaction, payment, or account number change, do you manually check the bank details provided are correct through another channel (i.e. by phone) before actioning such request?	Yes ☐	No ☐

5. Response and Recovery

5.1 Backing up Data

a)	Do you take backups of key server configurations and data at least weekly?	Yes ☐	No ☐
b)	Are backups encrypted?	Yes ☐	No ☐
c)	Are backups disconnected and inaccessible through the organisation's network? (e.g. offsite or in a cloud)	Yes ☐	No ☐

d)	Do you test restoration and recovery of key server configurations and data from backups?	Yes ☐	No ☐

Why are off-site backups important? If you experience a security incident and availability to your data is compromised (i.e. encrypted with ransomware) restoring your data from backups may be able to get you back to business as usual and potentially avoid paying a ransom to get the data decrypted.

Why are we asking these questions? Ransomware remains a prolific attack vector for malicious actors. Successfully retrieving data from backups can avoid significant downtime, costs to recreate data or being in a position where you feel you need to pay a ransom to recover the data. However, backups are not a full proof plan to ransomware attacks. Modern forms of ransomware attacks are utilising data exfiltration as opposed to just encryption methods providing attackers a secondary path to extortion in the event you can successfully recover from backups.

Want to undertake more research on backups? For more information on backups see the advisory by CERT NZ here

5.2 Log Management

a)	Have you enabled log management for your organisation to alert unusual or unexpected events within your technology environment?	Yes ☐	No ☐

What is log management? Log management is the methodology that involves consistently collecting, preserving, handling, consolidating, and examining data. This practice aims to enhance system efficiency, detect technical problems, efficiently allocate resources, fortify security measures, and promote adherence to regulatory standards.

Why are we asking this question? Even with excellent cybersecurity hygiene you are not immune from attack. Should an attack occur IT security teams can analyse these logs to trace the origin of an attack, identify the methods used by the attackers, and understand the extent of the compromise.

Want to undertake more research on setting up of logs? For more information on setting up logs see the advisory by CERT NZ here

5.3 Response Planning

a) Are the following plans implemented:			Frequency of review		Date of last audit/test
Business Continuity Plan (BCP)	Yes ☐	No ☐	Monthly ☐	Yearly ☐	
Disaster Recovery Plan (DRP	Yes ☐	No ☐	Monthly ☐	Yearly ☐	

What is a response plan for cyber specific scenarios? Digital assets and your online systems are critical to running your day-to-day operations. As we become more reliant on technology the criticality only increases. It is therefore important to have a plan prepared in case things go wrong not just for our physical environments but also for our digital environments. Having a response plan in the event of a cyber event may save time in response and therefore cost to the business and its reputation.

Why are we asking these questions? We want to ensure you are prepared for a cyber scenario should something go wrong. This can save time for mitigation response and recovery which in turn can lead to less downtime and therefore impact and/or cost to the business and its stakeholders.

Want to undertake more research on incident response plans? For more information on incident response plans see the advisory by CERT NZ here

Declaration

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

1. 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.
2. this proposal and declaration shall be the basis of and incorporated in the insurance contract.
3. 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.
4. 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.

Please Note:

- **Completion of this proposal does not bind the Applicant or Vero Liability to enter into a contract of insurance.**
- **The information and explanations provided on this proposal is provided for general information only.**
- **Vero Liability does not assume any responsibility for giving legal or other professional advice and disclaims any liability arising from the use of the information and explanations.**
- **If you require legal or other expert advice you should seek assistance from a professional adviser.**

Vero Liability Insurance Limited
Level 32 ANZ Centre, 23-29 Albert Street
Private Bag 92055, Auckland 1142, New Zealand
Telephone 09 306 0350

Print Form