CHUBB®

Cyber Enterprise Risk Management

Short MarketPlace Cyber Proposal Form

Important

Claims-Made and Claims-Made and Notified Coverages
These coverages apply only to claims that are either first made against you during the period of insurance or both first made against you and notified to us in writing before the expiration of the period of the insurance cover provided by your policy. If your Policy does not have a continuity of cover provision or provide retrospective cover then your Policy may not provide insurance cover in relation to events that occurred before the contract was entered into.

Completing This Proposal Form

- Please read the Important Information Section on page 6 before completing this form.
- Please contact us if you would like a hard copy of the relevant insurance policy or a summary of cover provided by Chubb.
- **This Proposal Form is for Businesses with revenue of Less than $50m.**
- It is agreed that whenever used in this Proposal Form, the term "You" and "Your" shall mean the Named Insured and all its Subsidiaries.
- Certain words appearing in green bold font have a certain meaning as per the glossary section below.
- This document allows Chubb to gather the needed information to assess the risks related to your information systems. If your information systems security policies differ between your companies or subsidiaries, please complete separate proposal forms for each information system.

I. Company Information

Named Insured:	
Address:	
Year Established:	
Number of Employees:	
Website:	
Industry:	Professional Services
Business Description:	

Total Revenue:	
Percentage of revenue generated from the US:	

II. Underwriting Questions

1. Does the client currently or will the client potentially operate in any of the following?

☐ Accreditation Services	☐ Government and/or Local Regional Authority
☐ Adult Content	☐ Manufacturer of Life Safety Products or Services
☐ Credit Bureau	☐ Media Production
☐ Cryptocurrency Exchange or Distributed Ledger Technology	☐ Payment Processing or Trading Exchanges
☐ Cybersecurity Product or Services	☐ Peer to Peer File Sharing
☐ Data Aggregation / Brokerage / Warehousing	☐ Social Media Platform
☐ Financial Institution	☐ Surveillance (Physical or Digital)
☐ Gambling Industry	☐ Third Party Claims Administration
☐ Technology and IT Managed Services	☐ None of these

2. Does any part of your network (including email, corporate and/or OT systems) maintain remote access capability?	☐ Yes ☐ No
If Yes, is **Multi-Factor Authentication** required for all remote network access capability?	☐ Yes ☐ No

3. Please confirm if your backups for mission critical systems are protected by the following:

- ☐ immutable or write-once read-many protections
- ☐ access to backups is restricted via **multi-factor authentication**
- ☐ completely offline or air-gapped (tape or nonmounted disk) that is disconnected from the rest of your network
- ☐ access to backups is restricted via separate privileged accounts that are not connected to active directory or other domains
- ☐ None of these

4. Please confirm which of the following endpoint protection technologies are in place on all laptops, desktops, and servers:

- ☐ **URL or web filtering**
- ☐ **Application isolation and containment**
- ☐ **Centralised Endpoint Protection Platform**
- ☐ Advanced antimalware and antivirus with heuristic capabilities
- ☐ **EDR (endpoint detection and response), XDR (extended detection and response), or MDR (managed detection and response)**
- ☐ None of these

5. Please confirm which of the following email security measures are in place:

☐ Quarantine service for suspicious emails	☐ Ability to detonate attachments and links in a sandbox
☐ **Sender Policy Framework (SPF)** is enforced	☐ Phishing simulations or training for employees
☐ Microsoft Office macros are disabled on documents by default	☐ None of these

6. Does the possible maximum number of people you would be required to notify in case of a breach of **Personally Identifiable Information (PII)** exceed 500,000?	☐ Yes ☐ No
7. Do you, or your outsourced service provider, accept payment card transactions?	☐ Yes ☐ No
8. Are you compliant to the level of **PCI DSS** that applies to your company?	☐ Yes ☐ No
9. To the best of your knowledge, do you comply with all relevant privacy laws and regulations in the jurisdictions in which you operate?	☐ Yes ☐ No

II. Underwriting Questions *continued*

10. Is the client a subsidiary, franchisee, or smaller entity of a larger organisation?	☐ Yes ☐ No
If Yes, please provide additional details, including information about any Network interconnectivity and/or Segmentation:	

11. Does the Applicant:	
a) derive any revenue from Russia, Belarus, or Ukraine (including Crimea and the Luhansk and Donetsk regions);	☐ Yes ☐ No
b) have any operations, products, subsidiaries, employees, property or facilities in Russia, Belarus, or Ukraine (including Crimea and the Luhansk and Donetsk regions); or	☐ Yes ☐ No
c) have any supply chain reliance on companies or resources located in Russia, Belarus, or Ukraine (including Crimea and the Luhansk and Donetsk regions)?	☐ Yes ☐ No

12. Within the last 3 years, have you had any cyber incidents, known cyber events or become aware of any matter that could lead to a claim under a cyber insurance policy?	☐ Yes ☐ No
If Yes, please provide additional details, including how the incident occurred, total costs incurred and mitigation steps implemented post incident:	

13. Has the Applicant's Cyber or Technology insurance submission previously been declined by Chubb, or is Chubb currently the insurer for either policy?	☐ Yes ☐ No
If Yes, please provide additional details, including the Policy Number if Chubb is currently the insurer:	

I confirm that the information declared herein is a true and correct declaration of my client/the policyholder's completed proposal form and that I have obtained a declaration to that effect from my client, which I am able to produce if requested to do so.

14. Please provide contact details for the client's Chief Information Security Officer or other staff member who is responsible for data and network security:

Role/Title:	
First Name:	
Last Name:	
Email Address:	
Phone Number:	

III. Optional Coverage Extension - Social Engineering Fraud

1. Does the Applicant currently purchase or intend to purchase any Social Engineering Fraud coverage through Chubb or another carrier under a separate policy?	☐ Yes ☐ No
2. Do you require that all outgoing payments or funds transfers be subject to segregations of duties between initiation and authorisation, such that no one individual can control the entire process?	☐ Yes ☐ No
3. Do you require that all outgoing payments or funds transfers be subject to dual authorisation by at least one supervisor after being initiated by a third employee?	☐ Yes ☐ No
4. Do you confirm all changes to vendor/supplier details (including routing numbers, account numbers, telephone numbers, and contact information) by a direct call using only the contract number previously provided by the vendor/ supplier before the request was received?	☐ Yes ☐ No

IV. Declaration

The undersigned authorised officers of the named Insured declare that to the best of their knowledge and belief the statements made in this proposal and in all attachments and schedules to this proposal are true and are true and notice will be given as soon as practicable should any of the above information change between the date of this proposal and the proposed date of inception of the insurance. Although the signing of the proposal does not bind the undersigned, on behalf of the Named Insured, to effect insurance, the undersigned agree that this proposal and all attachments and schedules to this proposal and the said statements in this proposal shall be the basis of and will be incorporated in the policy should one be issued.

The undersigned, on behalf of the Named Insured and all of its subsidiaries, acknowledge that the Statutory Notice contained in this proposal has been read and understood.

Name of Director, Officer or Risk Manager:	
Signature:	
Date:	

Glossary of Defined Terms

Application Isolation & Containment - this technology can block, restrict, or isolate specific endpoints from performing potentially harmful actions between endpoints and other applications or resources with the goal to limit the impact of a compromised system or endpoint.

Centralised Endpoint Protection Platform - is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Endpoint Detection and Response (EDR) - is a solution which records and stores endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems.

Extended Detection and Response (XDR) - is a security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components, typically including endpoints, networks, servers, cloud services, SIEM, and more.

Managed Detection and Response (MDR) - is a managed cyber security service that provides intrusion detection of malware and malicious activity in your network, and assists in rapid incident response to eliminate those threats with succinct remediation actions.

Multi-Factor Authentication (MFA) - MFA is an electronic authentication method used to ensure only authorised individuals have access to specific systems or data. A user is required to present two or more factors - these factors being 1) something you know, 2) something you have, or 3) something you are. Something you know may include your password or a pin code. Something you have may include a physical device such as a laptop, mobile device that generates a unique code or receives a voice call or a text message, a security token (USB stick or hardware token), or a unique certificate or token on another device. Something you are may include biometric identifiers.

- Note that the following are not considered secure second factors: a shared secret key, an IP or MAC address, a VPN, a monthly reauthentication procedure, or VOIP authentication.

PCI DSS - PCI DSS stands for the Payment Card Industry Data Security Standard. This defines the requirements that a company must comply with if they handle any payment card information.

Personally Identifiable Information (PII) - means any data that can be used to identify a specific individual. This may include health or medical records of employees or customers, government issued identification numbers, login usernames, email addresses, credit card numbers, biometric information, and other related personal information.

Sender Policy Framework (SPF) - is an email authentication method that is used to prevent unauthorised individuals from sending email messages from your domain, and generally helps to protect email users and recipients from spam and other potentially dangerous emails.

URL Filtering or Web Filtering - is technology that restricts which websites a user or browser can visit on their computer, typically filtering out known malicious or vulnerable websites.

Important Information

In this section "We", "Our" and "Us" means Chubb Insurance New Zealand Limited (Chubb). "You" and "Your" refers to Our customers and prospective customers as well as those who use Our website.

Duty of Disclosure

Your Duty of Disclosure

Before entering into a contract of insurance with Chubb, each prospective insured has a duty to disclose to Chubb information that is material to Chubb's decision whether to accept the insurance and, if so, on what terms. This includes material information about the insured, any other people and all property and risks insured under the policy. Information may be material whether or not a specific question is asked.

There is the same duty to disclose material information to Chubb before renewal, extension, variation or reinstatement of a contract of insurance with Chubb. You should also provide all material information when You make a claim or if circumstances change during the term of the contract of insurance.

It is important that each prospective insured understands all information provided in support of the application for insurance and that it is correct, as each prospective insured will be bound by the answers and by the information they have provided.

The duty of disclosure continues after the application for insurance has been completed up until the time the contract of insurance is entered into.

Consequences of Non-Disclosure

If an insured fails to comply with their duty of disclosure, Chubb may be entitled, without prejudice to its other rights, to reduce its liability under the contract in respect of a claim or refuse to pay the entire claim. Chubb may also have the right to avoid the contract from its beginning. This means the contract will be treated as if it never existed and no claims will be payable.

Financial Strength Rating

At the time of print, Chubb has an "AA-" insurer financial strength rating given by S&P Global Ratings. The rating scale is:

The rating scale is:			
AAA Extremely Strong	BBB Good	CCC Very Weak	SD or D Selective default or default
AA Very Strong	BB Marginal	CC Extremely Weak	R Regulatory Action
A Strong	B Weak		NR Not Rated

The rating from 'AA' to 'CCC' may be modified by the addition of a plus (+) or minus (-) sign to show relative standings within the major rating categories. A full description of the rating scale is available on the S&P Global Ratings website.

Our rating is reviewed annually and may change from time to time, so please refer to Our website for Our latest financial strength rating.

Fair Insurance Code

We are a member of the Insurance Council of New Zealand (**ICNZ**) and a signatory to ICNZ's Fair Insurance Code (**the Code**). The Code and information about the Code is available at www.icnz.org.nz and on request.

Privacy Statement

This statement is a summary of Our privacy policy and provides an overview of how We collect, disclose and handle Your personal information.
Our privacy policy may change from time to time and where this occurs, the updated privacy policy will be posted on Our website.

Chubb is committed to protecting Your privacy. Chubb collects, uses and retains Your personal information in accordance with the requirements
of New Zealand's Privacy Act, as amended or replaced from time to time.

Personal Information Handling Practices

When do We collect Your personal information?
Chubb collects Your personal information (which may include health information) from You when You interact with Us, including when You are applying for, changing or renewing an insurance policy with Us or when We are processing a claim, complaint or dispute. Chubb may also (and You authorise Chubb to) collect Your personal information from other parties such as brokers or service providers, as detailed in Our privacy policy.

Purpose of Collection
We collect and hold the information to offer products and services to You, including to assess applications for insurance, to provide and administer insurance products and services, and to handle any claim, complaint or dispute that may be made under a policy.

If You do not provide Us with this information, We may not be able to provide You or Your organisation with insurance or to respond to any claim, complaint or dispute, or offer other products and services to You or Your organisation.

Sometimes, We may also use Your personal information for Our marketing campaigns and research, to improve Our services or in relation to new products, services or information that may be of interest to You.

Recipients of the Information and Disclosure
We may disclose the information We collect to third parties, including:

- contractors and contracted service providers engaged by Us to deliver Our services or carry out certain business activities on Our behalf (such as actuaries, loss adjusters, claims investigators, claims handlers, professional advisers including lawyers, doctors and other medical service providers, credit reference bureaus and call centres);
- intermediaries and service providers engaged by You (such as current or previous brokers, travel agencies and airlines);
- other companies in the Chubb group;
- the policyholder (where the insured person is not the policyholder);
- insurance and reinsurance intermediaries, other insurers, Our reinsurers, marketing agencies; and
- government agencies or organisations (where We are required to by law or otherwise).

These third parties may be located outside New Zealand. In such circumstances We also take steps to ensure Your personal information remains adequately protected.

From time to time, We may use Your personal information to send You offers or information regarding Our products that may be of interest to You. If You do not wish to receive such information, please contact Our Privacy Officer using the contact details provided below.

Rights of Access to, and Correction of, Information
If You would like to access a copy of Your personal information, or to correct or update Your personal information, want to withdraw Your consent to receiving offers of products or services from Us or persons We have an association with, please contact the Privacy Officer by posting correspondence
to Chubb Insurance New Zealand Limited, PO Box 734, Auckland; telephoning: +64 (9) 3771459; or emailing Privacy.NZ@chubb.com.

How to Make a Complaint
If You have a complaint or would like more information about how We manage Your Personal Information, please review Our Privacy Policy for more details, or contact Our Privacy Officer at the details above.

You also have a right to address Your complaint directly to the Privacy Commissioner by telephoning 0800 803 909, emailing enquiries@privacy.org.nz or using the online form available on the Privacy Commissioner's website at www.privacy.org.nz.

About Chubb in New Zealand

Chubb is the world's largest publicly traded property and casualty insurer. Chubb's operation in New Zealand (Chubb Insurance New Zealand Limited) offers corporate Property & Casualty, Group Personal Accident and corporate Travel Insurance products through brokers.

More information can be found at www.chubb.com/nz.

Contact Us

Chubb Insurance New Zealand Limited
CU1-3, Shed 24
Princes Wharf
Auckland 1010
PO Box 734, Auckland 1140
O +64 9 377 1459
F +64 9 303 1909
www.chubb.com/nz

Company No. 104656
Financial Services Provider No. 35924

Chubb. Insured.℠