CYBEREDGE®

AN IMPORTANT NOTICE

The CyberEdge Policy is issued / insured by AIG Insurance New Zealand Limited (AIG), Company Number: 3195589, FSP: 189804, a licensed insurer regulated by the Reserve Bank of New Zealand.

Auckland: The AIG Building, Level 19, 41 Shortland Street, Auckland, New Zealand 1140

Contact numbers: +64 9 355 3100

YOUR DUTY OF DISCLOSURE

Before you enter into an insurance contract, you have a duty to disclose to AIG anything that you know, or could reasonably be expected to know, is relevant to AIG's decision whether to accept the risk of the insurance and, if so, on what terms.

You have this duty until we agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell us anything that:

- diminishes the risk we insure you for; or
- is common knowledge; or
- we know or, in the ordinary course of business ought to know as an insurer; or
- we waive your duty to tell us about.

Subject to the Cancellation General Provision, if you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both.

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

CLAIMS-MADE AND NOTIFIED

The Third Party Liability Section of the CyberEdge Policy and some Optional Extensions contain claims-made and notified Insuring Clauses. This means that those Insuring Clauses will only cover Claims first made against you during the Cyber Edge Policy Period and notified to the Insurer as soon as practicable in the CyberEdge Policy Period or any applicable extended reporting period. The CyberEdge Policy may not provide cover for any Claims made against you if at any time prior to the commencement of the CyberEdge Policy you became aware of facts which might give rise to those claims being made against you.

The CyberEdge Policy excludes prior **Insured Events**, **Claims** and circumstances as outlined in the Exclusion 4.14 (Prior **Insured Events**, **Claims** and circumstance.

This notice sets out how AIG collects, uses and discloses personal information about:

- you, if an individual; and
- other individuals you provide information about.

Further information about our Privacy Policy is available at www.aig.co.nz or by contacting us at privacy.officerNZ@aig.com.

HOW WE COLLECT YOUR PERSONAL INFORMATION

AIG usually collects personal information from you or your agents.

AIG may also collect personal information from:

- our agents and service providers;
- other insurers;

- people who are involved in a claim or assist us in investigating or processing claims, including third parties claiming under your policy, witnesses and medical practitioners;
- third parties who may be arranging insurance cover for a group that you are a part of;
- providers of marketing lists and industry databases; and
- publically available sources.

WHY WE COLLECT YOUR PERSONAL INFORMATION

AIG collects information necessary to:

- underwrite and administer your insurance cover;
- improve customer service and products and carry out research and analysis, including data analytics; and
- advise you of our and other products and services that may interest you.

You have a legal obligation to disclose certain information. Failure to disclose information required may result in AIG avoiding the contract from the beginning.

The **Insurer** complies with the Information Privacy Principles. The Information Privacy Principles apply to any personal information collected by the **Insurer.**

Purpose of collection

The **Insurer** collects personal information about **You** for the purposes of assessing **Your** application for insurance and administering **Your** policy. Failure to provide relevant personal information may result in the **Insurer** not being able to administer **Your** policy, process any **Claim** under **Your** policy or **You** may breach **Your** duty of disclosure.

TO WHOM WE DISCLOSE YOUR PERSONAL INFORMATION

In the course of underwriting and administering your policy we may disclose your information to:

- your or our agents, entities to which AIG is related, reinsurers, contractors or third party providers providing services related to the administration of your policy;
- banks and financial institutions for purpose of processing your application for insurance and obtaining policy payments;
- your or our agents, assessors, lawyers, vendors, third party administrators, emergency providers, retailers, medical providers, travel carriers, in the event of a claim;
- entities to which AIG is related and third party providers for data analytics functions whether in New Zealand or overseas;
- other entities to enable them to offer their products or services to you; and
- government, law enforcement, dispute resolution, statutory or regulatory bodies, or as required by law.
- **Breach Coach** and associated service providers under this policy in order to enable them to complete pre-screening on Insured pursuant to the Anti Money Laundering and Countering Financing of Terrorism Act 2009.

AIG is likely to disclose information to some of these entities located overseas, including in the following countries: United States of America, Canada, Bermuda, United Kingdom, Ireland, Belgium, The Netherlands, Germany, France, Singapore, Malaysia, the Philippines, India, Hong Kong, Australia as well as any country in which you have a claim and such other countries as may be notified in our Privacy Policy from time to time.

You may request not to receive direct marketing communications from AIG.

The **Insurer** will only disclose **Your** personal information to these parties for the primary purpose for which it was collected or to enable the Insurer to advise **You** of its insurance products or services. In some circumstances the **Insurer** is entitled to disclose **Your** personal information to third parties without Your authorisation such as law enforcement agencies or government authorities.

ACCESS TO YOUR PERSONAL INFORMATION

You may gain access to your information by submitting a written request to AIG. In some circumstances AIG may not permit access to your personal information. Circumstances where access may be denied include where it would compromise the privacy of other individuals or where it would be unlawful.

AIG has also established an internal dispute resolution process for handling customer complaints and an access and correction procedure. Both procedures are generally free of charge however AIG reserves the right to charge for access requests in limited circumstances.

If you feel you have a complaint about AIG's information privacy principles, require assistance in lodging a privacy complaint or you wish to gain access to your information, you may write to:

The Privacy Manager
AIG Insurance New Zealand Limited
PO Box 1745, Shortland Street, Auckland 1140
(64) 9355 3100

Your complaint will be reviewed and you will be provided with a written response. If it cannot be resolved, your complaint will be referred to the Internal Disputes Resolution Committee who will respond within 15 business days. In either case the matter will be reviewed by a person or persons with appropriate authority to deal with the complaint. Should your complaint not be resolved by AIG's internal dispute resolution process, you may take your complaint to the Privacy Commissioner for review of the determination.

CONSENT

If applicable, your application includes a consent that you and any other individuals you provide information about consent to the collection, use and disclosure of personal information as set out in this notice.

COPYRIGHT

The content of this Policy, including but not limited to the text and images herein, and their arrangement, is the copyright property of AIG. All rights reserved. AIG hereby authorises you to copy and display the content herein, but only in connection with AIG business. Any copy you make must include this copyright notice. Limited quotations from the content are permitted if properly attributed to AIG; however, except as set forth above, you may not copy or display for redistribution to third parties any portion of the content of this Policy without the prior written permission of AIG. No modifications of the content may be made. Nothing contained herein shall be construed as conferring by implication or otherwise any license or right under any patent, trademark, copyright (except as expressly provided above), or other proprietary rights of AIG or of any third party.

FAIR INSURANCE CODE

AIG is a signatory to the Fair Insurance Code. This Code aims to raise the standards of practice and service in the insurance industry, improve the way that claims and complaints are handled and help people better understand how general insurance works. You can obtain a copy from www.icnz.org.nz or by contacting AIG.

DISPUTE RESOLUTION PROCESS

We are committed to handling any complaints about our products or services efficiently and fairly.
If you have a complaint:

(i) contact your insurance intermediary and they may raise it with us;
(ii) if your complaint is not satisfactorily resolved you may request that your matter be reviewed by management by writing to:

The Complaints Manager
AIG Insurance New Zealand Limited
PO Box 1745, Shortland Street, Auckland 1140

(iii) if you are still unhappy, you may request that the matter be reviewed by the **Insurer's** Internal Dispute Resolution Committee. We will respond to you with the Committee's findings within 15 business days.
(iv) if you are not satisfied with the finding of the Committee, you may be able to take your matter to the insurance industry's independent dispute resolution body. This external dispute resolution body can make decisions with which we are obliged to comply.

GENERAL INFORMATION

1. Name of Organisation:

2. Principle address:

3. Date of establishment:

4. Have any mergers or acquisitions taken place in the last 5 Years? ☐ Yes ☐ No

   If 'Yes', please provide details, including how processes, policies and procedures have been integrated with the main group:

5. Are there planned Mergers or Acquisitions for the next 12 months? ☐ Yes ☐ No

6. Are you involved in any joint ventures? ☐ Yes ☐ No

   If 'Yes', please provide details including how processes, policies and procedures have been integrated with the main group:

7. Please provide an overview of your business activities:

8. Please state the number of employees:

9. Please complete the following revenue table:

   Currency:

Revenue Amount			
Geography	**Last Complete Year (Actual)**	**Current Year (Estimate)**	**Next Year (Estimate)**
New Zealand			
Australia			
UK / Europe			
USA / Canada			
Rest of World			

DATA PROTECTION EXPOSURE

1. Please state the number of data records currently processed/stored in the following categories:

	UK/Europe		US/Canada		Rest of World	
	Processed	Stored	Processed	Stored	Processed	Stored
Basic Personal Information						
Sensitive Personal Information						
Payment Card Information						
Financial Account Information						
Health Related Information						
Employee Personal Information						
3rd Party Corporate Information						

2. Is customer/client information shared with 3rd parties? ☐ Yes ☐ No

If 'Yes':

a. Who is data shared with and for what purpose?

b. Are you indemnified for breaches of the data by such 3rd parties? ☐ Yes ☐ No

c. Is data always anonymized/aggregated prior to release? ☐ Yes ☐ No

d. Where data is not anonymized, do you always seek permission from the data subject prior to release? ☐ Yes ☐ No

NETWORK INTERRUPTION EXPOSURE

Section to be completed only if the proposer is looking to purchase Network Interruption cover

1. Please provide a split of your revenue / income streams:

a. Online sales %

b. Offline sales %

c. Brokerage / commission %

d. Unit / usage fees %

e. Contract / subscription / licensing fees %

f. Professional / service fees %

g. Lending / renting / leasing %

h. Investment income %

i. Donations %

j. Grants %

2. In what way would revenue be impacted following a disruption to or failure of your computer system, network or applications (please include estimates of lost revenue, 3rd party liability and customer churn)?

3. Please outline any seasonal peaks in revenue, including the relevant percentage increase:

4. Please state the time after which disruption would lead to a reduction in net revenue:

5. Please describe actions taken to prevent outages from occurring, including usage of backup power systems, fault tolerant architecture, excess bandwidth for multiple providers, etc.:

6. Please describe the actions you would take to mitigate the duration of such disruption if it were to occur, including details of any operational and system failover measures:

7. Please describe the actions you would take, including the likely costs associated with such actions, in order to mitigate the impact of a material interruption. examples of such costs may include additional staffing / overtime opening additional contact centres or re-housing IT equipment / servers / data centres or making customer compensation payments:

8. Do you have formal business continuity / disaster recovery plans? ☐ Yes ☐ No

   If 'Yes':

   a. What are the recovery time objectives for system restoration?

   b. How often are such plans tested?

9. Do you have a formal change management control policy including risk assessment, testing, authorization, change control procedures and roll back procedures for major systems?

10. Do you have a lifecycle management process for assessing and replacing system/network equipment?

Outsourcing Exposure

Section to be completed only if the proposer outsources IT / Data services to third parties

1. Please state all IT / Data services that are outsourced to third parties, including cloud providers (please use a separate sheet if required):

Service	Vendor Name:	On demand service (incl. Infrastructure, Platform or Software as a Service models)
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No

2. What due diligence is undertaken before engaging with a new outsourced service provider (OSP)?

3. Do you have a process for regular security audits on OSPs? ☐ Yes ☐ No

4. Where data is processed or stored by 3rd party providers, how do you assess and manage the risks posed by shared infrastructure such as clouds or shared servers?

5. For all on-demand services, is data stored in a private cloud? ☐ Yes ☐ No

If 'No', to what extent are public clouds used and how is access to data controlled?

6. If a data breach occurs, which party incurs the costs of notification and what is the OSP's obligation in this situation?

7. If an OSP system or cloud service is unavailable, what is the likely impact on you?

8. What contractual indemnities are in place in the event of a data breach or network unavailability caused/suffered by the OSP or cloud provider?

9. How do your business continuity and/or disaster recovery plans address an OSP or cloud failure?

DATA SECURITY

1. Have you designated a Chief Privacy Officer? ☐ Yes ☐ No

   If 'No', please explain how this function is monitored and controlled within your organisation and who is responsible:

2. Do you have a group-wide privacy policy? ☐ Yes ☐ No

   If 'Yes', are you in compliance with it? ☐ Yes ☐ No

3. When was the privacy policy last reviewed and by whom?

4. Does the privacy policy comply with the privacy legislation applicable to all jurisdiction and industry standards and requirements, in which the company operates? ☐ Yes ☐ No

5. Do you have a data classification policy with adequate levels of security in place for sensitive data? ☐ Yes ☐ No

6. Is your network configured to ensure that access to sensitive data is limited to properly authorized requests, with privileges reviewed regularly? ☐ Yes ☐ No

7. Do you monitor access to sensitive information on your network? ☐ Yes ☐ No

8. Is all sensitive and confidential information stored on your database/servers and data files encrypted? ☐ Yes ☐ No

   If 'No', please describe the security measures (i.e. access control) in place to protect this information:

9. Is sensitive / confidential information encrypted in transmission? ☐ Yes ☐ No

10. Is critical data backed-up at least weekly? ☐ Yes ☐ No

11. Do you maintain your own back-up tapes/cassettes/disks etc.? ☐ Yes ☐ No

If 'Yes', are they stored in a physically secured location? ☐ Yes ☐ No

12. Please state your compliance with the following:

Service	Complaints?	If 'No', please provide details:
Payment Card Industry Data Security Standards	☐ Yes ☐ No ☐ N/A	
Please select Version	☐ 2.0 ☐ 3.0	
Please select Level	☐ 1 ☐ 2 ☐ 3 ☐ 4	
Other (Please Specify)	☐ Yes ☐ No ☐ N/A	

13. Please describe your data retention and destruction policy:

14. Do you have user revocation procedures on user accounts following employee termination? ☐ Yes ☐ No

NETWORK SECURITY

1. Do you utilize the following (please select all that apply)?

- ☐ Firewalls at the network
- ☐ Firewalls protecting sensitive resources kept inside the network
- ☐ Web application firewalls (WAF)
- ☐ Anti-Virus or Anti-Malware software that is updated or patched in accordance to vendor recommendations
- ☐ Intrusion detection
- ☐ Prevention systems
- ☐ Proactive vulnerability scanning
- ☐ If selected, do your vulnerability scans include web pages? ☐ Yes ☐ No
- ☐ Physical controls preventing access to the network
- ☐ Network access controls for remote access (e.g. VPN with 2 factor authentication)

2. Do you enforce a 'strong password policy' requiring passwords of adequate complexity and length, avoiding re-use for all accounts? ☐ Yes ☐ No

If 'No', please describe the measures in place to manage password security:

3. Do you carry out server and application security configuration hardening? ☐ Yes ☐ No

4. Does the organisation maintain a Whitelist to prevent malicious software and other unapproved programs for running? ☐ Yes ☐ No

   If 'No', do you apply the principle of least privilege to user rights? ☐ Yes ☐ No

5. Please describe your process for managing and installing patches on systems and applications (including any testing / due diligence phase prior to deployment):

6. Are you using any unsupported operating systems or software? ☐ Yes ☐ No

   If 'Yes', how do you plan to address this issue?

7. Do you have a formal change control policy which includes risk assessment, testing authorization, change control procedures and roll back procedures for major systems? ☐ Yes ☐ No

8. Do you backup critical systems more often than non-critical systems? ☐ Yes ☐ No

9. Do you allow BYOD? ☐ Yes ☐ No

   If Yes, how do you manage this risk? Please also include details regarding access control and remote device wiping:

10. Is write access to USB drives disabled for employees? ☐ Yes ☐ No

11. Please describe how you monitor and actively block advanced malware (which cannot be defected by traditional anti-virus software):

12. Does your organisation have a Social Media presence? ☐ Yes ☐ No

    If 'Yes', are all accounts 'user specific' rather than general administration accounts and how is social media activity monitored? ☐ Yes ☐ No

SECURITY POLICIES AND TESTING PROCEDURES

1. Do you maintain any certified information security standards? ☐ Yes ☐ No

   If 'Yes', please state (e.g. ISO27001):

2. Do you have a group-wide security policy, which is communicated to all employees? ☐ Yes ☐ No

3. Do you have a cyber-threat intelligence gathering function? ☐ Yes ☐ No

4. Is regular testing carried out by a 3rd party? ☐ Yes ☐ No

If 'Yes':

a. When was the last test performed?

b. Were any serious concerns raised in any aspect of the network? ☐ Yes ☐ No

c. Have concerns been addressed and successfully remediated? ☐ Yes ☐ No

5. Are regular security assessments carried out by a 3rd party? ☐ Yes ☐ No

If 'Yes':

a. When was the last assessment undertaken?

b. Were any serious concerns raised in any aspect of the network? ☐ Yes ☐ No

c. Have concerns been addressed and successfully remediated?

6. Do you have a continuous awareness training programme for employees regarding data privacy/security, including legal liability and social engineering issues? ☐ Yes ☐ No

If 'Yes', does this include any active social engineering testing (e.g. phishing) on employees? ☐ Yes ☐ No

7. Do you perform background verification checks for all candidates of employment, contractors and 3rd party users? ☐ Yes ☐ No

MERCHANTS, POINTS OF SALE AND TESTING PCI

1. Do you accept payment via Card-Present transaction? ☐ Yes ☐ No

If 'Yes':

a. Are you fully compliant with EMV card processing standards? ☐ Yes ☐ No

b. Do your POS systems have anti-tampering features? ☐ Yes ☐ No

c. Please describe the encryption and/or tokenization process of data flowing through your POS network, please include whether point-to-point encryption is used:

d. Do changes on individual files on the POS system create alerts in real-time? ☐ Yes ☐ No

e. Do changes to the POS systems require formal approval prior to implementation? ☐ Yes ☐ No

f. Are your POS devices regularly scanned for malware of skimming devices? ☐ Yes ☐ No

g. How often is your POS network assessed by a 3rd party?

h. Did you last POS network assessment highlight any critical or high level vulnerabilities? ☐ Yes ☐ No

If 'Yes', Have these been remediated? ☐ Yes ☐ No

i. Is your POS system developed and maintained by a PA-DSS compliant vendor? ☐ Yes ☐ No

j. Have all vendor-provided default passwords been charged? ☐ Yes ☐ No

k. Please describe how you segregate your POS and corporate network?

l. Is all user activity on the network monitored? ☐ Yes ☐ No

m. Is payment transaction log data collected and reviews on a regular basis? ☐ Yes ☐ No

2. Do you accept payment via Card-not-Present transactions? ☐ Yes ☐ No

If 'Yes':

a. Do you use 3rd party payment gateways to process payments? ☐ Yes ☐ No

b. Please describe how payment card data is captured and transferred to the credit card processor, including the encryption and/or tokenization process?

INCIDENT RESPONSE & CLAIMS HISTORY

1. Do you keep and incident log of all system security breaches and network failures? ☐ Yes ☐ No

If 'Yes', please describes the escalation and review process for such incidents:

2. Do you have an incident response plan which includes a team with specified roles and responsibilities? ☐ Yes ☐ No

If 'Yes', has this been tested within the last 12 months? ☐ Yes ☐ No

3. During the last 5 years, have you suffered from any of the following?

a) The unauthorized disclosure or transmission of any confidential information for which you are responsible ☐ Yes ☐ No

b) Any intrusion of, unauthorized access to, or unauthorized use of your computer system ☐ Yes ☐ No

c) Any accidental, negligence or unintentional act or failure to act by and employee or an employee of any third party service provider whilst operating, maintain or upgrading your computer system ☐ Yes ☐ No

d) The suspension or degradation of your computer system ☐ Yes ☐ No

e) Your inability to access data due to such data being deleted, damaged, corrupted, altered or lost ☐ Yes ☐ No

f) Receipt of an extortion demand or security threat ☐ Yes ☐ No

g) Receipt of a claim in respect of any of the above ☐ Yes ☐ No

h) Any formal or official action, investigation, inquiry or audit by a regulator arising out of your use, control, collection, storing, processing or suspected misuse of personal information ☐ Yes ☐ No

If 'Yes' to any of the above, please provide full details:

DECLARATION

Please Note: Signing the Declaration does not bind the proposer or the Insurer to complete this insurance.

I declare that I have made all necessary inquiries into the accuracy of the responses given in this proposal and confirm that the statements and particulars given in this proposal are true and complete and that no material facts have been omitted, misstated or suppressed. I agree that should any of the information given by me alter between the date of this proposal and the inception date of the insurance to which this proposal relates, I will give immediate notice thereof to the insurer.

I acknowledge receipt of the Important Notice, Privacy Notice and Disclosure information contained in this proposal and that I have read and understood the content of them.

I consent to AIG collecting, using and disclosing personal information as set out in AIG's privacy notice in this proposal and the policy.

If I have provided or will provide information to AIG about any other individuals, I confirm that I am authorised to disclose the other individual's personal information to AIG and also to give the above consent on both my and their behalf.

I confirm that I am authorised by the proposing company (and its partners/principals/directors if applicable) to complete this proposal form and to accept the quotation terms for this insurance on behalf of the company (and its partners/principals/directors if applicable)

Name:	
Title:	
Signature:	
Date:	

ABOUT AIG

AIG Insurance New Zealand Limited, a subsidiary of American International Group, Inc. (AIG). www.aig.co.nz. American International Group, Inc is a leading global insurance organisation. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, retirment products, and other financial services to customers in more than 80 countries and jurisdications. These diverse offerings include products and services the help businesses and individuals protect their assets, manage risks and provide for retirement security. American International Group, Inc common stock is list on the New York Stock Exchange and the Tokyo Stock Exchange.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products and services may not be available in all countries, and coverage is subject to actual policy language. Non-Insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insured are therefore not protected by such funds.