Proposal Form

CyberEdge®

Please find Important Notice and Disclaimers at the end of this document.

General Information

1. Name of Policyholder:
2. Principal Address:
3. Date of Establishment: / /
4. Policyholder Website:
5. 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:
6. Are there planned mergers or acquisitions for the next 12 months? ☐ Yes ☐ No
7. Are there any mergers or acquisitions planned to occur in the next 12 months? ☐ Yes ☐ No
   If 'Yes', please provide details including how processes, policies and procedures have been integrated with the main group:
8. Please provide an overview of your business activities:
9. Please complete the following revenue table:

	Prior Year	Current Year (Estimate)
Total Gross Revenue	$	$
Of the above, what amount of revenue is derived through on-line sales/service (e-commerce)	$	$
Geographical Split of Revenue (%)	$	$
Australia and NZ	$	$
United States	$	$
Rest of World	$	$

10. Annual IT Security Budget: $

Data Protection Exposure

11. Please state the number of data records currently processed/stored (by you or a third party) in the following categories:

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

12. Is customer/client information shared with third 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 third 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

13. 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, third party liability and customer churn)?

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

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

Application or Activity	Maximum time before reduction in revenue				
	<6 hrs	<12 hrs	<24 hrs	<48 hrs	>48 hrs

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

If 'Yes':

(a) What are the recovery time objectives (RTO) for critical system restoration?

☐ Under 5 hours ☐ Under 12 hours ☐ Under 24 hours ☐ Over 24 hours ☐ Other

(b) How often are such plans tested?

☐ Quarterly ☐ Semi-annually ☐ Annually ☐ Bi-annually ☐ Other or N/A

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

18. Do you operate, or anticipate operating any systems/applications or technology which are no longer supported by their vendor? ☐ Yes ☐ No

If 'Yes', what?

Outsourcing Exposure

19. Please detail all elements of your IT Operations outsourced to third Parties:

Outsourced Service		Service Provider	Who configures the settings?
Data Centre Hosting	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Managed Security	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Data Processing	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Payment Processing	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Application Service Provider	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Alert Monitoring Log	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Offsite Backup & Storage	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Cloud Computing	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
- Please detail service			
Network Management	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Desktop Management	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Server Management	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A
Other (please specify)	☐ Yes ☐ No		☐ Vendor ☐ User ☐ N/A

20. Do you require Outsourced Service Providers (OSPs) to maintain insurance or other means of indemnification for losses caused by the provider including privacy breach? ☐ Yes ☐ No

21. Have you entered into any Hold Harmless agreements, or otherwise waived any legal rights or entitlements you may have against any OSP? ☐ Yes ☐ No

22. How often do you review/audit engagement with OSPs?
☐ Annually ☐ Bi-annually ☐ Never ☐ Other (please detail)

23. Who in the company is responsible for assessing, appointing and managing OSP engagement?

24. If an OSP system or service suffers a failure, how soon before your operations are impacted?

OSP system or service	Maximum time before reduction in revenue				
	<6 hrs	<12 hrs	<24 hrs	<48 hrs	>48 hrs

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

Data Security

26. Have you designated a Chief Privacy Officer? ☐ Yes ☐ No
    If 'No', please explain how this function is monitored and controlled within your Company and who is responsible:

27. Do you have a group-wide privacy policy? ☐ Yes ☐ No
    If 'Yes', are you in compliance with it? ☐ Yes ☐ No

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

29. Have all employees undergone education and training in the privacy policy? ☐ Yes ☐ No

30. 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

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

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

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

34. How frequently do you back up critical data?
    ☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly ☐ Annually ☐ No backup is performed
    ☐ Other (please detail)

35. 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	

36. Please describe your data retention and destruction policy:

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

Network Security

38. Do you utilise 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)
    - ☐ Network Segmentation to separate critical areas from non-critical areas

39. 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:

40. Do you enforce Dual Factor Authentication for access to critical information and/or systems? ☐ Yes ☐ No

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

42. How long does the company take to install all vendor recommended security patches/updates?
    ☐ Under 30 days ☐ Over 30 Days ☐ We don't install patches

43. Does the company maintain a Whitelist to prevent malicious software and other unapproved programs from running? ☐ Yes ☐ No
    If 'No', do you apply the principle of least privilege to user rights? ☐ Yes ☐ No

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

45. 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:

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

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

48. Does your company have a Social Media presence? ☐ Yes ☐ No
    If 'Yes', are all accounts 'user specific' rather than general administration Accounts?

49. How is social media activity monitored?

Security Policies and Testing Procedures

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

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

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

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

53. Is regular penetration testing carried out by a third 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

54. Are regular security assessments carried out by a third 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? ☐ Yes ☐ No

55. 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

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

Merchants, Points Of Sale and testing PCI

57. 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 third party?

    (h) Did your 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

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

    If 'Yes':

    (a) Do you use third 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 and Claims History

59. 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:

60. 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

61. During the last 5 years, have you suffered from any of the following? ☐ Yes ☐ No

(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:

Stamp Duty Split

62. For the purpose of calculating Stamp Duty please state the number of current staff (including directors/partners, full/part time and casual employees) located in each state:

NSW	VIC	QLD	SA	WA	TAS	ACT	NT	Overseas
							Total of all employees	

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		Signature	
Title		Date	

About AIG

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, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. 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.

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.

Important Notices

This Policy is issued/insured by AIG Australia Limited (AIG), ABN 93 004 727 753 AFSL No 381686

Sydney: 2 Park Street, NSW 2000 (1300 030 886)
Melbourne: Level 13, 717 Bourke Street, VIC 3008 (1300 030 886)
Brisbane: 10 Eagle Street, QLD 4000 (1300 030 886)
Perth: 77 St. George's Terrace, WA 6000 (1300 030 886)

Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and 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:

- reduces the risk we insure you for; or
- is common knowledge; or
- we know or should 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

Some coverage sections of t*his policy contain claims-made and notified* insuring clauses. This means that those insuring clauses will only cover **Claims** first made against you during the **Policy Period** and notified to the **Insurer** as soon as practicable in the **Policy Period** or any applicable extended reporting period. This Policy may not provide cover for any **Claims** made against you if at any time prior to the commencement of this Policy you became aware of facts which might give rise to those claims being made against you.

Section 40(3) of the *Insurance Contracts Act 1984* provides that where you gave notice in writing to an insurer of facts that might give rise to a claim against you as soon as was reasonably practicable after you became aware of those facts but before insurance cover provided by an insurance contract expires, the insurer is not relieved of liability under the contract in respect of the claim, when made, by reason only that it was made after the expiration of the period of insurance cover provided by the contract.

This Policy excludes prior **Insured Events** (including but not limited to **Claims**) and circumstances as outlined in the "Prior Claims and Circiumstances" Exclusion in Section 10 of the Policy Wording.

Privacy Notice

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.com.au or by contacting us at australia.privacy.manager@aig.com or on 1300 030 886.

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 under the Insurance Contracts Act 1984 to disclose certain information. Failure to disclose information required may result in AIG declining cover, cancelling your insurance cover or reducing the level of cover, or declining claims.

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 policy payments;
- your or our agents, assessors, 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;
- 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.

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, New Zealand 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.

Access to Your Personal Information

Our Privacy Policy contains information about how you may access and seek correction of personal information we hold about you. In summary, you may gain access to your personal information by submitting a written request to AIG.

In some circumstances permitted under the Privacy Act 1988, AIG may not permit access to your personal information. Circumstances where access may be denied include where it would have an unreasonable impact on the privacy of other individuals, or where it would be unlawful.

Complaints

Our Privacy Policy also contains information about how you may complain about a breach of the applicable privacy principles and how we will deal with such a complaint.

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

Code of Practice

The **Insurer** is a signatory to the General Insurance Code of Practice. This 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. Information brochures on the Code are available upon request.

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 Compliance Manager
AIG Australia Limited
Level 13, 717 Bourke Street
Docklands VIC 3008