Proposal Form

CyberEdge®

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

General Information

1. Name of Company:
2. Principal Address:
3. Date of Establishment: / /
4. Company 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 (%)	$	$
Singapore	$	$
UK/Europe	$	$
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 3rd party) in the following categories:

	Singapore		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								
3rd Party Corporate Information								

12. 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

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, 3rd 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. Does Business Continuity Plan (BCP)/Disaster Recovery (DR) plan cover all business critical applications? ☐ Yes ☐ No

Network Interruption Exposure

17. 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

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

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

If 'Yes', what?

20. Do you have controls to protect from Distributed Denial Of Service (DDOS)? ☐ Yes ☐ No

If 'Yes', what?

Outsourcing Exposure

21. Please detail all elements of your IT Operations outsourced to 3rd 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

22. 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

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

24. How often do you review/audit engagement with OSPs?

☐ Annually ☐ Bi-annually ☐ Never ☐ Other (please detail)

Outsourcing Exposure

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

26. 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

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

Data Security

28. 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:

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

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

31. Have all employees undergone education and training into the privacy policy? ☐ Yes ☐ No

32. 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

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

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

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

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

37. Please state your compliance with the following:

Service	Compliance	If 'No', please provide details:
Payment Card Industry Data Security Standards	☐ Yes ☐ No ☐ N/A	
Please select Level	☐ 1 ☐ 2 ☐ 3 ☐ 4	

Network Security

38. Please describe your data retention and destruction policy:

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

40. 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
- ☐ Virtual Private Network (VPN) required to access corporate network remotely?
- ☐ VPN is configured with multi-factor authentication?
- ☐ Multi-Factor Authentication mandatory to access email remotely?
- ☐ Network Segmentation to separate critical areas from non-critical areas

41. Do you have process in place to identify rouge devices connected to corporate network? ☐ Yes ☐ No
If 'Yes', please provide further details below.

42. 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:

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

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

45. Do you maintain lists of all assets connected to the corporate network? ☐ Yes ☐ No
If 'Yes', Is the asset inventory validated at least annually? ☐ Yes ☐ No

46. 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

47. 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

48. 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

49. Do you allow Bring Your Own Device (BYOD)? ☐ Yes ☐ No
If Yes, how do you manage this risk? Please also include details regarding access control and remote device wiping:

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

Security Policies and Testing Procedures

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

52. Does your company have a social media presence? ☐ Yes ☐ No
    If 'Yes', are all accounts 'user specific' rather than general administration accounts?

53. How is social media activity monitored?

54. Do you maintain any certified information security standards? ☐ Yes ☐ No
    If 'Yes', please state (e.g. ISO27001):

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

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

57. Is regular penetration 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

58. 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? ☐ Yes ☐ No

59. 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

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

Policy & Testing Procedures

61. Is IT Risk Assessment conducted annually? ☐ Yes ☐ No

62. Is the output of IT Risk Assessment reviewed by executive management? ☐ Yes ☐ No

Digital Footprint

63. Please provide the range of public IP attributed to your organisation.

64. Please provide a list of domains / subdomains attributed to your organisation.

Merchants, Points Of Sale and Testing PCI

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

If 'Yes':

(a) Are you fully compliant with Europay, MasterCard and Visa (EMV) card processing standards? ☐ Yes ☐ No

(b) Do your Point Of Sale (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 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 Payment Application Data Security Standard (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

66. 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:

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

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

Incident Response and Claims History

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

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

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

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

(b) Any intrusion of, unauthorised access to, or unauthorised 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:

AIG Cyber Risk Consulting Services

AIG's CyberEdge policy provides our Insureds with a range of risk consulting services and preventative tools to provide cyber knowledge, training, security and consultative solutions. These services and tools add valuable layers to a company's line of defense. The services and tools available are:

- Employee Cybersecurity eLearning
- Phishing Simulator
- Blacklist IP Blocking and Domain Protection
- Infrastructure Vulnerability Scan
- Network Security Ratings Security Scorecard
- Cyber Maturity Report
- One-on-one session with AIG's Cyber Risk Consultant
- CyberEdge Claims Hotline

Please provide a contact's email address for our Cyber Risk Consultant to contact you regarding these tools and services:

Declaration

The undersigned, authorised to sign and bind on behalf of the company, hereby declares that the statements and particulars in this Proposal Form are true and no material facts have been misstated or suppressed. A material fact is one that would influence the acceptance or assessment of the risk.

The undersigned agrees that this Proposal Form, and any attachment or information submitted therewith and any and all other information supplied or requested, shall form the basis of any insurance agreement effected thereon. The undersigned further undertakes to inform the insurer of any material alteration to any information, statements, representations or facts presented in this proposal form, occurring before or after the inception date of the insurance agreement.

This Proposal Form is binding on the company and will form the basis of the data protection insurance policy concluded with AIG Asia Pacific Insurance Pte. Ltd.

I agree and consent, and if I am submitting information relating to another individual, I represent and warrant that I have authority to provide that information to AIG, I have informed the individual about the purposes for which his/her personal information is collected, used and disclosed as well as the parties to whom such personal information may be disclosed by AIG, as set out in the contents of the consent claused contained below and the individual agrees and consents, that AIG may collect, use and process my/his/her personal information (whether obtained in this application form or otherwise obtained) and disclose such information to the following, whether in or outside of Singapore: (i) AIG's group companies; (ii) AIG's (or AIG's group companies') service providers, reinsurers, agents, distributors, business partners; (iii) brokers, my/his/her authorised agents or representatives, legal process participants and their advisors, other financial institutions; (iv) governmental / regulatory authorities, industry associations, courts, other alternative dispute resolution forums, for the purposes stated in AIG's Data Privacy Policy which include:

a) Processing, underwriting, administering and managing my/his/her relationship with AIG;
b) Audit, compliance, investigation and inspection purposes and handling regulatory / governmental enquiries;
c) Compliance with legal or regulatory obligations, risk management procedures and AIG internal policies;
d) Managing AIG's infrastructure and business operations; and
e) Carrying out market research and analysis and satisfaction surveys.

Note: Please refer to (and if submitting information relating to another individual, refer such individual to) the full version of AIG's Data Privacy Policy found at **https://www.aig.sg/privacy** before you provide your consent, and/or the above representation and warranty.

Acceptance of this Proposal Form does not constitute an agreement by AIG Asia Pacific Insurance Pte. Ltd. to bind this policy. It is subject to review and approval by AIG Asia Pacific Insurance Pte. Ltd.

The undersigned confirms to have been fully informed about all coverage details including all applicable sublimits. He/she further confirms to have recieved, carefully read and understood the standard data protection insurance policy wording.

Name

Title

Date

Signature

Note to the Proposer

Signing or completing this proposal does not bind the Proposer, or any individual or entity he or she is representing to complete the insurance.

Please provide, by addendum, any supplementary information which is material to the response of the questions herein, and/or complete answers to the listed questions if they do not fit in the space provided on the application.

For the purpose of this proposal form, "Proposer" means the entity stated in 1. above and all its subsidiaries to be covered.

All answers should be given as a group response, i.e. if any subsidiary company has different responses these should be provided separately on your headed paper.

Important Notice

Statement pursuant to Section 25(5) of the Insurance Act (Cap 142) or any amendments thereof: you are to disclose in the application, fully and faithfully, all the facts which you know or ought to know, otherwise the policy issued may be void and you may receive nothing from the policy.

The requirement in Section 25(5) of the Insurance Act is set out for your compliance:

No Singapore insurer shall use, in the course of carrying on insurance business in Singapore, a form of proposal which does not have prominently displayed therein a warning that if a proposer does not fully and faithfully give the facts as he knows them or ought to know them, he may receive nothing from the policy.

About AIG

American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference herein.

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 or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and 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 insureds are therefore not protected by such funds.