AIG

CyberEdge

Proposal Form

Bring on tomorrow

CyberEdge: Proposal Form

A. 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)
UK / Europe			
USA/Canada			
Rest of World			

B. Data 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 anonymised/aggregated prior to release? .... □ Yes □ No

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

3. Do you ensure that data is not transferred to any territory unless such territory has an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data? .... □ Yes □ No

C. 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 .... %

   k. Other (please advise) .... %

2. In what way would revenue/profit 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 profit:

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? .... □ Yes □ No

10. Do you have a lifecycle management process for assessing and replacing system/network equipment? .... □ Yes □ No

D. 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 (including 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?

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

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

5. Do you monitor access to sensitive information on your network? .... □ Yes □ No

6. Is all sensitive and confidential information stored on your databases/servers and data files encrypted? .... □ Yes □ No

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

7. Is sensitive / confidential information encrypted in transmission? .... □ Yes □ No

8. Is all critical data backed-up at least weekly? .... □ Yes □ No

9. 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

10. Please state your compliance with the following:

	Compliant?	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	
Fair and Accurate Credit Transactions Act (FACTA)	□ Yes □ No □ N/A	
Health Information Portability and Accountability Act (HIPAA)	□ Yes □ No □ N/A	
Health Information Technology for Economic and Clinical Health Act (HITECH)	□ Yes □ No □ N/A	
Gramm-Leach Bliley Act (1999)	□ Yes □ No □ N/A	
Other (Please Specify)	□ Yes □ No □ N/A	

11. Please describe your data retention and destruction policy:

12. Do you have user revocation procedures on user accounts following employee termination? .... □ Yes □ No

AIG

F. Network Security

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

   □ Firewalls at the network Perimeter

   □ 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 or prevention systems

   □ Proactive vulnerability scanning.

   If selected, do your vulnerability scans include all 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 from 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, authorisation, 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 detected 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

G. 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 t
   o all employees? .... □ Yes □ No

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

4. 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?

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

H. Merchants, Points of Sale and PCI

Section to be completed only if the proposer accepts payment by card

1. Do you accept payment via Card-Present transactions? .... □ 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 tokenisation 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 or 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 PA-DSS compliant vendor? .... □ Yes □ No

j. Have all vendor-provided default passwords been changed? .... □ 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 tokenisation process?

I. Incident Response and Claims History

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

   If 'Yes', please describe 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?

   The unauthorised disclosure or transmission of any confidential information for which you are responsible .... □ Yes □ No

   Any intrusion of, unauthorised access to, or unauthorised use of your computer system .... □ Yes □ No

   Any accidental, negligent or unintentional act or failure to act by an employee or an employee of any third party service provider whilst operating, maintaining or upgrading your computer system .... □ Yes □ No

   The suspension or degradation of your computer system.................................. □ Yes □ No

   Your inability to access data due to such data being deleted, damaged, corrupted, altered or lost.. □ Yes □ No

   Receipt of an extortion demand or security threat... □ Yes □ No

   Receipt of a claim in respect of any of the above... □ Yes □ No

   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

It is declared that to the best of the knowledge and belief of the insured, after enquiry, that the statements and responses set out herein are true and accurate. The insured understands that it is under a duty to make a fair presentation of the risk to the insurer, and that all material circumstances that the insured is aware of or ought to be aware of have been disclosed to the insurer, or failing that, sufficient information to put a prudent insurer on notice that further enquiries are needed.

The insured understands that non-disclosure or misrepresentation of a material fact or matter may impact the terms of the policy or impact whether the policy responds in whole or in part to a claim.

The insured undertakes to inform the Insurers of any material alteration to the information provided herein or any new fact or matter that arises which may be relevant to the consideration of the proposal for insurance.

(to be signed by Partner, Director, Principal or equivalent)

Signed ____

Title ____

Organisation ____

Date ____

AIG Europe Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 202628). This information can be checked by visiting the FS Register (www.fsa.gov.uk/register/home.do).AIG Europe Limited is a member of the Association of British Insurers. Registered in England: company number 1486260. Registered address: The AIG Building, 58 Fenchurch Street, London, EC3M 4AB.