OBF

INSURANCE GROUP

CYBER

PROPOSAL FORM

Coverholder at

LLOYD'S

OBF Insurance Group Ltd. Bridge House, Baggot Street Bridge, Dublin 4. D04 X2P1
T: +353 1 660 1033 / 676 0201 | F: +353 1 668 7985 | E: piteam@obf.ie | W: www.obf.ie

Please Note:

- This is a proposal for a contract of insurance, in which 'proposer' or 'you/your' means the individual, company, partnership, limited liability partnership, organisation or association proposing cover.

- This proposal must be fully completed, signed and dated. All questions must be answered to enable a quotation to be given but completion does not bind you or the insurer to enter into any contract of insurance.

- If there is insufficient space to answer any questions fully, please attach a signed continuation sheet. You should retain a copy of the completed proposal (and of any other supporting information) for future reference.

- OBF Insurance Group Ltd. draws your attention to the importance of answering all questions honestly and with reasonable care. The answers you give us must be true and complete. This is for your protection because, if you do not give us full and complete information, a claim under your policy could be declined or your cover cancelled. You should also advise us of any material changes in your circumstances which might alter the subject matter of the policy or the nature of the risk being insured. If you do not advise us of such changes, cover under the policy may be lost.

- You are recommended to request a specimen copy of the proposed policy wording from your insurance broker and to consider carefully the terms, conditions, limitations and exclusions applicable to the cover.

DETAILS OF THE PROPOSER

1. Name(s) of the Firm(s):

2. Address(es):

3. Website:

4. Email address:

5. Phone No:

6. Establishment Date of Firm:

7. Locations of Overseas Offices (Please list Countries):

8. Please state total number of: Principals/Partners/Directors: Employees:

9. a) Describe in detail your business activities:

b) Do you anticipate any changes in those activities in the forthcoming 12 months? Yes No
If Yes, please provide full details:

c) Is the company part of any professional body or association? Yes No
If Yes, please provide full details:

d) Does the company possess any professional accreditation? Yes No
If Yes, please provide full details:

DETAILS OF INCOME/FEES

1. a) Please provide the details of your gross fees:

	Last Financial Year / /	Current Financial Year / /	Estimate for Next Financial Year / /
Gross Fee			
Maximum Fee			
Average Fee			

b) Financial Year End:

2. a) Please provide a percentage split of your income by geographical area:

	% of Gross Fees
Domestic Contracts (Ireland)	
UK Contracts	
EU Contracts (excluding Ireland and UK)	
USA/Canada (Subject to non USA/Canada Law)	
USA/Canada (Subject to USA/Canada Law)	
Rest of the World Contracts (Please list countries)	

b) Please provide an approximate breakdown of your revenues by client type:

Corporate/(B2B): Consumer/(B2C):

DETAILS OF PEOPLE

1. Can you confirm you adhere to the following best practices:

a) Have a dedicated individual responsible for information security and privacy? Yes No N/A

b) Perform background checks on all employees and contractors with access to sensitive data? Yes No N/A

c) Perform background checks on all employees and contractors whose work involves critical IT infrastructure? Yes No N/A

d) Have restricted access to sensitive data (including physical records) to only those requiring it? Yes No N/A

e) Have a process to delete systems access within 48 hours after employee termination? Yes No N/A

f) Have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training? Yes No N/A

If NO to any of the above, please detail below along with mitigating comments:

2. Have you terminated the contract of any IT staff members in the last 12 months? Yes ☐ No ☐

If Yes, how many and which titles did they hold?

If Yes, were any of these decisions made as a result of malicious or dishonest actions? Yes ☐ No ☐

If Yes, please provide more information:

DETAILS OF WEBSITE

1. Please detail your website functionality:

Tick if applicable

a) Basic brochure website ☐

b) Third party advertising on your website ☐

c) User content allowed (chat rooms, bulletin boards, discussion forums etc) ☐

d) Large content volumes published ☐

e) Large media download / streaming volumes ☐

f) Client log-in area ☐

g) Transactional, accepting payments (card, Paypal etc) ☐

2. Does your website allow third parties to post comments or connect directly to your website? Yes ☐ No ☐

If Yes, do you offer a mechanism for website viewers to flag content they are unhappy with? Yes ☐ No ☐

Describe how you manage such issues when brought to your attention:

3. What percentage of your turnover emanates from online or e-commerce activities? %

4. Typically, how often is your website changed in terms of content or functionality?

Tick most applicable

a) Regularly (at least every few days) ☐

b) Weekly or monthly ☐

c) Sporadically / when needed (not typically more than once per month) ☐

d) Are changes checked by a second person before "go live"? Yes ☐ No ☐

DETAILS OF NETWORK

1. If your IT network failed, which of the following would best describe the impact to your business?

a) Inconvenience, very minimal revenue impact and operations could continue temporarily ☐

b) Revenues would NOT be impacted immediately, and only slightly when impacted ☐

c) Revenues would NOT be impacted immediately, but significantly when impacted ☐

d) Revenues would be impacted immediately but only slightly ☐

e) Revenues would be impacted immediately and significantly ☐

f) Operations and revenues would be entirely interrupted ☐

Please describe further:

2. Can you confirm you comply with the following minimum security standards:

(a) You use anti-virus, anti-spyware and anti-malware software? Yes ☐ No ☐

b) You use firewalls and other security appliances between the internet and sensitive data? Yes ☐ No ☐

(c) You use intrusion detection or intrusion prevention systems (IDS/IPS) and these are monitored? Yes ☐ No ☐

(d) You perform regular backups and periodically monitor the quality of the backups? Yes ☐ No ☐

If No to any of the above, please detail below along with mitigating comments:

3. In which timescales do you update anti-virus / anti-malware protections with patches?
Tick if applicable:

a) As soon as practicable but always promptly, directly following patch release? ☐

b) Weekly or monthly? ☐

c) Once per week? ☐

d) Less often than weekly (please detail timescale)?

4. a) Please provide details of the vendors for the following services:
(or check box if it is managed and operated in-house):

	Vendor	In-house
Internet service provider		
Cloud / Hosting / Data centre provider		
Payment processing		
Offsite archiving backup and storage		
Data or information processing (such as marketing or payroll)		

b). Do you typically require such outsourced providers to:

Demonstrate adequacy of IT security and risk management procedures? Yes ☐ No ☐

Procure and evidence relevant insurance for the services they provide to you? Yes ☐ No ☐

c) Indemnify you contractually in respect of their errors or negligence (including data breach and system downtime)? Yes ☐ No ☐

If No to any of the above, why not?

5. a) Do you have a written "data breach" or "privacy breach" response plan? Yes ☐ No ☐

b) Has this plan been tested? Yes ☐ No ☐

c) Last date of test or regularity of testing?

6. Do you only use operating systems that continue to be supported by the original provider? Yes ☐ No ☐

If No, please detail below along with mitigating comments:

7. Do you allow remote access to your network?

a) No ☐

b) Yes, to employees only ☐

c) Yes, to employees and other third parties ☐

If Yes, what security measures are utilised to keep such remote access secure?

8. a) What is the size of your dedicated IT budget annually?

b) Approx. proportion dedicated to IT security?

c) Has this gone up or down in the past 3 years? Up ☐ Down ☐

9. Are any major network / system IT changes envisaged or planned in the next 12 months? Yes ☐ No ☐

If Yes, please detail fully:

10. Are annual or more frequent internal/external audit reviews (including penetration testing) performed on your IT network and your procedures? Yes ☐ No ☐

If Yes, please provide a copy of the latest report from any examination/audit.

11. a) Do you have a disaster recovery plan (DRP) and/or business continuity plan (BCP) in place? Yes ☐ No ☐

b) In your DRP / BCP, how long would it take for you to be fully operational again following an incident?

c) How often do you test your DRP / BCP?

d) When did you last test your DRP / BCP?

12. Do you hold any of the following cyber / IT Security accreditations?

a) UK Government "Cyber Essentials" certified? Yes ☐ No ☐

b) ISO27001 Yes ☐ No ☐

c) PCI DSS (latest version)? Yes ☐ No ☐ N/A ☐

d) Which PCI Merchant Level are you?

Other accreditations held:

DETAILS OF DATA

1. Do you hold or process any of the following types of sensitive consumer data?

a) Financial information? (including credit/debit card records) Yes ☐ No ☐ Number of Records:

b) Medical information? Yes ☐ No ☐ Number of Records:

c) Identity information? (including National Insurance number or passport details) Yes ☐ No ☐ Number of Records:

d) Names, addresses, telephone numbers? Yes ☐ No ☐ Number of Records:

2. Do you hold or process any of the following types of sensitive corporate data:

a) Confidential intellectual property/trade secrets? Yes ☐ No ☐ Number of Records:

b) Financial information? Yes ☐ No ☐ Number of Records:

3. Do you utilise encryption in the following scenarios:

a) Sensitive data is encrypted at rest within your network? Yes ☐ No ☐

b) Sensitive data is encrypted on backup tapes? Yes ☐ No ☐

c) Sensitive data is encrypted when transmitted outside of your network? Yes ☐ No ☐

d) Sensitive data is encrypted when transferred to portable media devices (USBs, Laptops etc)? Yes ☐ No ☐

If No to any of the above, please provide mitigating comments:

4. Do you monitor, restrict or block employees' ability to remove data via network end-points such as USB drives? Yes ☐ No ☐

5. Do you have controls in place to restrict or control employees' ability to take physical data such as paper files away from your premises? Yes ☐ No ☐

6. Please detail any salting or hashing techniques, or any other type of password cryptography you use?

PREVIOUS/CURRENT INSURANCE

1. Does the Proposer currently have a Cyber Insurance policy in force? Yes ☐ No ☐

If Yes:

a) Insurer

b) Expiry Date

c) Limit of Indemnity

d) Excess

e) Premium

f) Expiry Retroactive Date

2. Has any previous policy for Cyber insurance been cancelled or refused or had any special terms imposed by any insurer? Yes ☐ No ☐

If Yes, please provide full details:

3. Please indicate the Limit of Indemnity required:

€500,000 ☐ €1,000,000 ☐ €1,500,000 ☐ €2,000,000 ☐ €2,500,000 ☐

€3,000,000 ☐ €5,000,000 ☐

Please specify if other:

4. What Excess is the Proposer prepared to carry uninsured?

€1,000, €2,500, €5,000, €10,000 or 'Other'

CLAIMS/CIRCUMSTANCES INFORMATION

1. Regarding all the types of insurance covers to which this proposal form relates, are you or any of the partners, principals, or directors, after having made full enquiries, including of all staff, aware of any of the following matters:

a) Any claims (successful or otherwise) or cease and desist orders being made against the company, its predecessors or present or past partners, principals, or directors? Yes ☐ No ☐

b) Any circumstances which may give rise to a claim against the company, its predecessors or any past or present partner, director, principal or employee? Yes ☐ No ☐

c) Any loss or damage that has occurred to the company or its predecessors? Yes ☐ No ☐

e) Any privacy breach, virus, DDOS, or hacking incident which has, or could, adversely impact(ed) your business? Yes ☐ No ☐

e) Any evidence of network intrusion or vulnerabilities highlighted in an IT Security audit or penetration test which have not yet been resolved? Yes ☐ No ☐

f) Any unforeseen down time to your website or IT network of more than 3 hours? Yes ☐ No ☐

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

2. Are there any other Material facts which ought to be disclosed? Yes ☐ No ☐
If Yes, please provide full details on a separate sheet.

DATA PROTECTION

OBF Insurance Group Ltd. recognise that protecting personal information including sensitive personal information is very important and we recognise that you have an interest in how we collect, use and share such information. Our Data Protection Policy is in line with the requirements under the General Data Protection Regulations (GDPR) which are effective from 25 May 2018.

Please read the following carefully as it contains important information relating to the information that you give us or has been provided to us on your behalf. If you provide information relating to anyone other than yourself, you are responsible for obtaining their consent to the use of their data in the manner outlined below.

Full details of how we collect, use, store and protect your data can be found in our Data Privacy Notice, a copy of which is available on request or via our website, www.obf.ie.

What does OBF Insurance Group Ltd. do with your personal data?

Information you provide will be used by OBF Insurance Group Ltd. for the purposes of processing your application and administering your insurance policy. OBF Insurance Group Ltd. may need to collect sensitive personal data relating to you (such as medical or health records) in order to process your application and/or any claim made.

All information supplied by you will be treated in confidence by OBF Insurance Group Ltd. and will not be disclosed to any third parties except (a) to our agents, sub-contractors and reinsurers (b) to third parties involved in the assessment, administration or investigation of a claim (c) where your consent has been received or (d) to meet our

legal or regulatory obligations. In order to provide you with products and services this information will be held in the data systems of OBF Insurance Group Ltd. or our agents or subcontractors. The data is held on servers with multiple layers of security. Please note that some servers which may hold your data are located outside the EU.

We will hold data collected from you for the duration of our business relationship with you and for six years after that. This is a requirement under the Central Bank's Consumer Protection Code 2012. Your data may be used for the purposes of automated decision making but will not be used for profiling purposes.

OBF Insurance Group Ltd. may pass your information to other companies for processing on its behalf. OBF Insurance Group Ltd. will ensure that its transfer of data is lawful and that your information is kept securely and only used for the purpose for which it was provided.

Calls to and from OBF Insurance Group Ltd. are recorded for quality assurance or verification purposes.

Your Rights under our Data Protection Policy

You have the right to :

- Access the data we hold about you
- Have the data we hold about you transferred to another person or organisation
- Have inaccurate data about you corrected
- Have information about you erased (this could affect our ability to process your business)
- Object to direct marketing from us
- Restrict the processing of your data (this could affect our ability to process your business)
- Make a complaint to us about the implementation of our data protection policy and procedures.

To access the data we hold about you, you will need to complete and submit a Data Access Request Form, available on request or via our website.

Data Breaches

In the event of a data breach which results in your personal data being compromised, we will advise the Data Protection Commissioner within 72 hours at most, unless the data was encrypted or anonymised. Were there is a high risk to your rights, as set out in the GDPR, we will also advise you of the details of the breach and the steps we have taken to rectify it and prevent its recurrence.

Fraud Prevention, Detection and Claims History

In order to prevent and detect fraud as well as the non-disclosure of material information, and in addition to comply with money-laundering legislation, OBF Insurance Group Ltd. may at any time:

- Share information about you with companies or organisations outside OBF Insurance Group Ltd. including, where appropriate, private investigators and public bodies including An Garda Siochana
- Check your details with fraud prevention agencies as well as databases and other sources of information including, but not limited to, the insurance industry claims database known as InsuranceLink. For information on the functioning of InsuranceLink, please visit insurancelink.ie.

DECLARATION

The undersigned authorised person declares that all questions in this Proposal Form have been answered honestly and with reasonable care and that no information which we requested has been withheld or misrepresented. He/she understands that non-disclosure of material information could result in a claim under the policy being declined. The undersigned agrees that, should any material information change between the date of this proposal and the inception date of the insurance to which this proposal relates, they will advise us thereof. The undersigned agrees that this proposal, together with any other material information supplied to us, shall form the basis of any contract of insurance effected thereon.

Signature:

Name:

Position:

Date: