MPR | MANAGEMENT & PROFESSIONAL RISKS

Cyber Incident Response and Insurance

Proposal Form

To be solid, insurance must be flexible.

Cyber Incident Response and Insurance

Note to the Applicant: Signing or completing this proposal does not bind the Applicant, or any individual or entity he or she is representing, to complete this insurance. Please provide by addendum any supplementary information which is material to the response of the questions herein. All answers should be given as a group response i.e. if any subsidiary company has different responses, these should be provided separately.

Policyholder Details

1. (a) Policyholder:
   (b) Other entities to be covered:

Name	Country of registration	Ownership/relationship

2. Address:

3. Website address:
4. How long has the policyholder continuously carried on business?
5. Number of employees:
6. Description of business activities (including those of any entities mentioned in Q1b):

7. During the last five years:
   (a) has the name of the policyholder or is business activities changed? Yes No
   (b) any acquisition or merger taken place? Yes No
   If 'Yes', please provide additional details below or by attachment.

8. Do you anticipate any major changes to the business activities or company structure in the next 12 months? Yes No
   If 'Yes', please provide additional details below or by attachment.

9. Are you currently accredited with any Information security standards (including Cyber Essentials, ISO 27001:2013, or others)? Yes No
   If 'Yes', please provide additional details below or by attachment.

10. Do you have a Data Privacy Officer or Chief Information Officer, who is responsible for your obligations under Data Protection and Privacy legislation? Yes No

11. In the last 12 months, have you had a third-party network security audit/assessment, or penetration-test of your network? Yes No

Cyber Incident Response and Insurance

General Information

12. Income Details:

(a) What is the revenue for the last 3 years and estimated fees for forthcoming year?

	20_____	20_____	20_____	(Estimated) 20____
UK (including ROI)	£	£	£	£
Europe	£	£	£	£
USA	£	£	£	£
Elsewhere	£	£	£	£
Total	**£**	**£**	**£**	**£**

13. (a) Percentage of revenue generated by online sales or operations: %

(b) Approximate breakdown of revenues by client type

Corporate/B2B	**Consumer/B2C**	**Average Transaction Value**
%	%	£

14. Personal Information

(a) Please circle/indicate the most appropriate range of records containing an individual's personal information processed, transmitted or stored per year.

0 – 10,000	**10,001 – 25,000**	**25,001 – 50,000**	**50,001 – 100,000**
100,001 – 250,000	**250,001 – 500,000**	**500,001 – 1,000,000**	**Over 1,000,000**

(b) If over 1,000,000 please advise a total:

15. Payment Cards

(a) Do you (or a third-party service provider on your behalf) accept payment card transactions? Yes No

(b) If 'Yes', are you compliant with the most recent applicable Payment Card Industry Data Security Standards (PCI DSS)? Yes No

If 'Yes', to what certification level (level 1-4)?

When was your last assessment?

(c) If the card payment process is outsourced, please confirm which level of self-assessment has been completed:

Please also confirm that you obtain a certificate of PCI-compliance annually from providers: Yes No

Cyber Incident Response and Insurance

16. Please advise/estimate by ticking the appropriate boxes:

	Up to 6h	6-12h	12-24h	24h+
How long does it take to restore your operations after a site or systems loss?				
How long would it be, following the inability of staff to access the computer network and systems, before there is a significant impact to your business?				

Risk Management - People

17.	(a)	Do you restrict access to sensitive data (including physical records) to only those requiring it?	Yes	No
		Does this include privileged user access and segregation of sensitive roles?	Yes	No
	(b)	Do you have a procedure to delete systems access and log-in credentials immediately following an employee's departure?	Yes	No
	(c)	Do you have a fully implemented staff training program in place for all employees regarding data privacy and information security?	Yes	No
	(d)	Do you perform background checks on the following?		
		i. All employees and contractors with access to sensitive data?	Yes	No
		ii. All employees and contractors who work on critical IT infrastructure?	Yes	No
	(e)	Do you allow remote access to your network?	Yes	No
		If 'Yes', do you have a VPN two-step authentication for remote access users?	Yes	No
	(f)	Do you monitor, restrict or block employee's ability to remove data from network end-points?	Yes	No
		If 'No' to any of the above, or there are other risk management features you wish to advise of, please provide details below or by attachment.		

Risk Management – Access & Security controls

18.	(a)	Do you track and monitor all access to sensitive information on your network and maintain a good history of logs?	Yes	No
	(b)	Do you enforce strong passwords for all users of systems providing access to personal/confidential information?	Yes	No
	(c)	Do you regularly update your security patches to your systems and applications?	Yes	No
	(d)	Do you have anti-virus and malware protection on all computer devices, servers and networks (that are updated/patched regularly?)	Yes	No
	(e)	Do you have firewalls/intrusion detection and network segregation to reduce the probability of complete outage?	Yes	No
		If 'Yes', are these monitored regularly with receipt and action of vulnerability alerts?	Yes	No

Cyber Incident Response and Insurance

(f) Please circle/indicate where you use encryption to protect sensitive and confidential data on your systems?

Databases	File storage/document sharing	Laptops
Mobile devices	External memory/Storage devices	Back-ups

(g)	Do you have a Mobile Device Management (MDM) System?	Yes	No
(h)	Do you back up your mission critical systems and data (to a different location, that is isolated from your network) at least weekly?	Yes	No
(i)	Do you only use operating systems that continue to be supported by the original supplier?	Yes	No

If 'No', please provide additional information:

What systems are unsupported and what are they used for?

Do they have an 'air-gap' from all unsecured networks (including LAN)?

(j)	Do you ensure that business technologies are maintained at the latest, or immediately previous, version?	Yes	No
(k)	Do you regularly scan your network for weaknesses or vulnerabilities?	Yes	No
(l)	Does access to critical information systems require multi-factor authentication?	Yes	No
(m)	Do you have multi-factor authentication for your email system (to protect against BEC - Business Email Compromise)?	Yes	No

If 'No' to any of the above, or there are other risk management features you wish to advise of, please provide details below or by attachment.

Risk Management - Outsourcing

19. (a) Please describe the functions that you outsource:

(b)	Do you require all third-party service providers (that you outsource your data processing, back up or hosting) to demonstrate their IT system resilience?	N/A	Yes	No
(c)	Do your outsourcing contracts include security requirements that should be observed by the third-party service provider?	N/A	Yes	No
(d)	Do your third-party service providers indemnify you contractually in respect of their errors or negligence, including data breaches?	N/A	Yes	No
(e)	Is your third-party service provider obligated to assist you in the investigation/recovery of a cyber incident?	N/A	Yes	No
(f)	Please confirm you have not waived your rights of recourse against the third-party service provider in the outsourcing contract	N/A	Yes	No

If 'No' to any of the above, or there are other risk management features you wish to advise of, please provide details below or by attachment.

Risk Management - Policies

20.	(a)	Do you have a policy to destroy data and documents no longer needed?	Yes	No
	(b)	Do you have a BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan), that are tested and updated regularly?	Yes	No
		If 'No', please provide additional information on the current process/procedure for incident response/business continuity (in relation to a cyber event).		
	(c)	Do you have a formal written privacy policy, reviewed and approved by management?	Yes	No
	(d)	Do you have a formal, written information security policy which is reviewed annually and communicated to all employees?	Yes	No

If 'No' to any of the above, or there are other risk management features you wish to advise of, please provide details below or by attachment.

Risk Management – Cyber Crime Controls

21	(a)	Does a Social Engineering Fraud risk management strategy exist and has the applicant informed and alerted relevant staff at all locations of Social Engineering Fraud (Social Engineering Fraud includes 'Fake President' fraud, payment diversion fraud and customer/manager impersonation fraud)?	Yes	No
	(b)	Do you have a process in place at all locations where unusual payment instructions purporting to come from the applicant's senior management are followed up by call backs to senior management at a previously known and pre-designated phone number to confirm payment instructions and check authenticity?	Yes	No
	(c)	Do you have a process in place at all locations where requests for authentication of bank account details or for information on bank account details purporting to come from bank officials are raised with the applicant's senior management and followed up with previously known bank contacts to confirm authenticity of such requests?	Yes	No
	(d)	Do you have a process in place at all locations where instructions to change bank account details purporting to come from vendors and suppliers are followed up by call backs to vendors and suppliers at a previously known and pre-designated phone number to confirm instructions to change bank account details and check authenticity?	Yes	No
	(e)	Do you have a process in place at all locations where senior management approval is always required before a change to beneficiary bank account details is processed, such approval being given after review of the underlying request and the record of its verification?	Yes	No
	(f)	Do you have a procedure to restrict telephone calls to premium rate numbers and/or notifications in the event of telephone bills exceeding financial caps?	Yes	No

If the answer to 20 (a), (b), (c), (d) or (e) is no, what controls do you apply?

Cyber Incident Response and Insurance

Loss Experience

22. Have you ever suffered a loss, whether insured or not, in respect of any of the risks to which this proposal for insurance relates? Yes No

If 'Yes', please provide a description below or by attachment, including date, location and amount of loss, as well as any preventative measures implemented.

23 (a) Are you aware of any circumstances which might lead to a claim, whether insured or not, in respect of any of the risks to which this proposal for insurance relates? Yes No

(b) In the last three years, are you aware of any cyber incidents or cyber events that have impacted the organisation? Yes No

If 'Yes', please provide a description below or by attachment.

Signature: _____

Date: _____

Name of Signatory: _____

Title of Signatory: Chairman of the Board / CEO / President/ Managing Director (delete as applicable)

Warning It is important that, when applying for the Policy, the applicants tell the insurers all facts which are material to the insurance. Failure to do so could wholly or partly invalidate the insurance. A material fact is one which might influence the insurers in deciding whether to accept the application or on what terms to insure. If in any doubt as to whether a fact is material, then the applicants should disclose it. They should keep a record (including copies of all letters and forms) of all information supplied to the insurers.