Cyber Insurance
Proposal Form

Important Notice

1. This is a proposal for a contract of insurance. You have a legal duty to provide a fair presentation of the risk. Failure to do so may make the contract of insurance voidable or severely prejudice your rights in the event of a claim.
2. This proposal must be completed signed and dated. All questions must be answered to enable a quotation to be given but completion does not bind you or insurers to enter into any contract of insurance. If space is insufficient 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.
3. 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.

Section A: General Information

1. (a) Name of company (insured)

   (b) Principal address

   (c) Postcode

   (d) Telephone

   (e) Date of establishment

   (f) Number of employees

   (g) Locations of overseas offices (please list countries)

2. (a) Describe in detail your business activities:

   (b) Do you anticipate any major changes in these activities in the forthcoming 12 months? Yes ☐ No ☐

   If YES, provide full details:

3. (a) Please detail your turnover, including fees, for the past year, and estimated turnover for the current and next year:

Date of your financial year end: | Currency:

	Past year	Current year (estimate)	Next year (estimate)
UK/Ireland			
Rest of Europe			
USA			
Rest of America			
Rest of the World (please list countries)			
Total			
Profit or (Loss)			

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

Corporate / B2B: % | Consumer / B2C %

4. Is the company part of any professional body or association? Yes ☐ No ☐

If YES, please detail below

5. Does the company possess any professional accreditation? Yes ☐ No ☐

If YES, please detail below

Section B: 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 ☐

(b) Perform background checks on all employees and contractors with access to sensitive data — Yes ☐ No ☐

(c) Perform background checks on all employees and contractors whose work involves critical IT infrastructure — Yes ☐ No ☐

(d) Have restricted access to sensitive data (including physical records) to only those requiring it — Yes ☐ No ☐

(e) Have a process to delete systems access within 48 hours after employee termination — Yes ☐ No ☐

(f) Have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training — Yes ☐ No ☐

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:

Section C: Website

1. Please list your website addresses and estimated current monthly unique visitors:

Website address	Estimated current monthly unique visitors

2. 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 payment cards ☐

3. Do you publish third party content on your website? Yes ☐ No ☐

If YES, do you have procedures in place, in respect of securing rights for using such content Yes ☐ No ☐

4. Does your website allow third parties to post comments or content 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:

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

6. 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 "put live"? Yes ☐ No ☐

Section D: 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 ☐

Less often than weekly (please detail timescale) ☐

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

		Vendor	In-house
(a)	Internet service provider		☐
(b)	Cloud / Hosting / Data centre provider		☐
(c)	Payment processing		☐
(d)	Data or information processing (such as marketing or payroll)		☐
(e)	Offsite archiving, backup and storage		☐

5. Do you typically require such outsourced providers to:

(a) Demonstrate adequacy of IT security and risk management procedures Yes ☐ No ☐

(b) 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?

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

(b) Have you tested this plan before? Yes ☐ No ☐

(c) Last date of test or regularity of testing? | |

7. 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:

8. Do you allow remote access to your network? No ☐

Yes, to employees only ☐

Yes, to employees and other third parties ☐

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

9. (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? | |

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

If YES, please detail fully

11. 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.

12. (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?

13. 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)? N/A ☐ Yes ☐ No ☐

(d) Which PCI Merchant Level are you?

Other accreditations held

14. Please describe your network contingency / redundancy / resilience in place to mitigate system interruptions or failures (such as mirrored infrastructure, failover mechanisms, warm or hot replicated sites or similar)?

Section E: Data

1. Do you hold or process any of the following types of sensitive CONSUMER data? Approx number of records

(a) Financial information (including credit/debit card records) Yes ☐ No ☐

(b) Medical information Yes ☐ No ☐

(c) Identity information (including NI number or passport details) Yes ☐ No ☐

(d) Names, addresses, telephone numbers Yes ☐ No ☐

1. Do you hold or process any of the following types of sensitive corporate data? Approx number of records

(a) Confidential intellectual property / trade secrets Yes ☐ No ☐

(b) Financial information Yes ☐ No ☐

2. 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

3. Do you segregate data to mitigate the risk of large scale data loss from a single intrusion? Yes ☐ No ☐

If YES, please provide full details

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?

Section F: Claims and Insurance History

1. Have you previously been insured for cyber risks? Yes ☐ No ☐

If YES, please provide the following unless you are currently insured with Markel

Limit of indemnity:		Insurer:	
Excess:		Expiry date:	
Premium:			

2. (a) Limit of indemnity required:

(b) Excess required:

3. 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 been made against the company, its predecessor, or present or past partners, principals, or directors Yes ☐ No ☐

(b) Any circumstances which may give rise to a claim against the company, its predecessor 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 predecessor Yes ☐ No ☐

(d) 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:

Declaration

I declare that I am authorised to complete this proposal and I confirm that, after appropriate enquiry, it is completed truthfully. I undertake to inform insurers of any alteration or addition to these statements or particulars which occur prior to the commencement of the period of insurance. It is hereby acknowledged and agreed that the terms, conditions, limitations and exclusions of the policy may be subject to alteration at any time prior to the commencement of the period of insurance should any such material alterations or additions arise. I also give consent to insurers to use the information. Signing of this proposal does not bind insurers to offer or the applicant to accept insurance.

Signed*	
Name	
Company position	
Date	

*the signatory should be a director or senior officer of, or a partner of, the company.

Your Personal Information

The basics

We collect and use relevant information about you to provide you with your insurance cover and to meet our legal obligations.
This information includes details such as your name and address and may include more sensitive details such as information about your health and any criminal convictions you may have.
The way insurance works means that your information may be shared with fraud prevention agencies and used by a number of third parties in the insurance sector – but only in connection with the insurance cover that we provide to you.

Other people's details you provide to us

Where you provide us with details about other people, you must provide this "**Your Personal Information**" notice to them.

Group policies

We will process individual insured's details, as well as any other personal information you provide to us in respect of your insurance cover, in accordance with our privacy notice and applicable data protection laws.
To enable us to use individual insured's details in accordance with applicable data protection laws, we need you to provide those individuals with certain information about how we will use their details in connection with your insurance cover.
You agree to provide to each individual insured this notice, on or before the date that the individual becomes an individual insured under your insurance cover or, if earlier, the date that you first provide information about the individual to us.
We are committed to only using the personal information we need to provide you with your insurance cover. To help us achieve this, you should only provide to us information about individual insureds that we ask for from time to time.

Want more details?

For more information about how we use your personal information please see our full Markel privacy notice, a copy of which is available online at http://www.markelinternational.com/foot/privacy-policy/ or on request.

Contacting us and your rights

You have rights in relation to the information we hold about you, including the right to access your information. Please contact us at dataprotectionofficer@markelintl.com or in writing to the Data Protection Officer, 20 Fenchurch Street, London, EC3M 3AZ if you wish to exercise your rights, discuss how we use your information or request a copy of our full Markel privacy notice.

NOTICE TO THE PROPOSER

The Underwriters
The underwriters will be either Markel International Insurance company Limited or Markel Syndicate 3000 at Lloyd's together with any other subscribing insurer(s).

Prior to any placement being concluded, the proposer will be advised which insurer(s) is/are to write this contract of insurance.

The Law of the Insurance Contract
The parties to this proposed insurance are free to choose the law applicable to the insurance contract. Unless specifically agreed otherwise with underwriters, the proposed contract will be governed by English law.

General Enquiries
If at any time you have any questions or concerns about your policy or the handling of a claim you should, in the first instance, contact Claims Manager, Professional Liability Division, 20 Fenchurch Street, London EC3M 3AZ.

Complaints Procedures

Markel Syndicate 3000
If you are insured by Markel Syndicate 3000 and in the event that you remain dissatisfied and wish to make a complaint, you can do so at any time by referring the matter to the Compliance Officer, Markel Syndicate Management Limited (Lloyd's Managing Agent for Syndicate 3000), 20 Fenchurch Street, London EC3M 3AZ or the Policyholder and Market Assistance Team at Lloyd's.

Their address is:
Policyholder and Market Assistance, Market Services, Lloyd's, One Lime Street, London, EC3M 7HA
Tel: 020 7327 5693 Fax: 020 7327 5225 e-mail: complaints@lloyds.com.

Details of Lloyd's complaints procedures are set out in a leaflet "Your Complaint – How We Can Help" available at www.lloyds.com/complaints and also available from the above address.

If you remain dissatisfied after Lloyd's has considered your complaint, you may have the right to refer your complaint to the Financial Ombudsman Service.

Following this complaints procedure does not affect your right to take legal action or to any other remedy available to you.

The Financial Ombudsman Service's contact details are:
Financial Ombudsman Service, Exchange Tower, Harbour Exchange Square, London, E14 9SR
website: www.financial-ombudsman.org.uk email: complaint.info@financial-ombudsman.org.uk
phone: 0800 023 4567 or 0300 123 9123

Markel Syndicate 3000 at Lloyd's of London
Markel Syndicate 3000 is a syndicate at Lloyd's of London. The Lloyd's Managing Agent for Markel Syndicate 3000 is Markel Syndicate Management Limited, registered in England and Wales, with its registered office at 20 Fenchurch Street, London EC3M 3AZ. Markel Syndicate Management Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (Financial Services Register No.: 204953).

Markel International Insurance Company Limited
If you are insured by Markel International Insurance Company Limited and in the event that you remain dissatisfied and wish to make a complaint, you can do so at any time by referring the matter to the Compliance Officer, Markel International Insurance Company Limited, 20 Fenchurch Street, London EC3M 3AZ.

If you are not satisfied with our final response to your complaint, you may have the right to refer the matter to the Financial Ombudsman Service without affecting your right to take legal action or to any other remedy available to you.

The Financial Ombudsman Service's contact details are:
Financial Ombudsman Service, Exchange Tower, Harbour Exchange Square, London, E14 9SR
website: www.financial-ombudsman.org.uk email: complaint.info@financial-ombudsman.org.uk
phone: 0800 023 4567 or 0300 123 9123

Markel International Insurance Company Limited
Markel International Insurance Company Limited, registered in England and Wales, with its registered office at 20 Fenchurch Street, London EC3M 3AZ. Markel International Insurance Company Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (Financial Services Register No.: 202570).