Markel Cyber 360
Application Form

Important Notice

1. This is an application 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 application must be completed **signed and dated within 30 days prior to inception**. 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 application (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) Postal code

   (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)
Canada			
USA			
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 %

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 or whose work involves critical IT infrastructure ☐ Yes ☐ No

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

(d) Have written information security policies and procedures that are reviewed annually and communicated to all employees ☐ Yes ☐ No

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

(e) Do you carry out employee information security awareness or data security training? Yes ☐ No ☐

If YES, what training is performed and how frequent is this performed?

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. 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 Security

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

(b) Approx. proportion dedicated to IT security?

(c) In percentage terms has this gone up or down in the last 3 years?

(d) Do you have an IT infrastructure lifecycle management process in place? Yes ☐ No ☐

If YES, please provide more information:

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 ☐

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

3. Do you perform regular backups and periodically monitor the quality of the backups? Yes ☐ No ☐

If YES, how regularly do you perform backups of your data (please tick):

☐ Daily ☐ Weekly ☐ Monthly ☐ Other

Where are these stored e.g. in the cloud, physical back up tapes. Please provide further details below.

4. How frequently 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) ☐

5. 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:

6. 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? E.g. Multi-factor authentication, VPNs

7. 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.

8. Do you hold any of the following cyber / professional accreditations?

   (a) ISO27001 N/A ☐ Yes ☐ No ☐

   (b) NIST Yes ☐ No ☐

   (c) Other accreditations held

Section E: Network Resilience

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. In terms of Cyber Business Interruption, please estimate your average revenue generated through your website or network?

   $ ☐ Daily ☐ Weekly ☐ Monthly

3. 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)? How frequently are these tested?

4. Please provide details of your Critical Service Providers (or check box if it is managed and operated in-house):

		Critical Service Providers	In-house
(a)	Internet service provider		☐
(b)	Cloud / Hosting / Data centre provider		☐
(c)	Payment processing		☐

(d) Any other critical service providers?

5. Do you typically require such critical service providers to:

(a) Demonstrate adequacy of their IT security and risk management procedures. Is this audited regularly? 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 ☐

Please provide further details on these controls

6. How often is vendor access rights reviewed and updated?

☐ Monthly ☐ Quarterly ☐ Annually Other

7. How is vendor access monitored on your network?

8. (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?

(e) Does your BCP/DRP consider critical service provider failure/issues and mitigate the risk? Yes ☐ No ☐

(f) Does your BCP/DRP consider outages to your IT network and infrastructure (system failures) and mitigate the risk? Yes ☐ No ☐

In respect of questions (e) and (f), please outline how these are tested?

9. Do you have any planned major upgrades / overhauls, system changes or similar over the next 12 months? Yes ☐ No ☐

If YES, what contingency plans are in place in case issues arise and is pre-launch testing carried out before go live? Please provide as much comfort as possible.

Section F: Data

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

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

(b) Payment card information (credit/debit card records) Yes ☐ No ☐

(c) Medical information Yes ☐ No ☐

(d) Identity information (including NI number, social security number or passport details) Yes ☐ No ☐

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

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

2. Are you subject to PCI-DSS? Yes ☐ No ☐

If yes, please provide the following details:

(a) What level of PCI Merchant are you?

(b) Are you compliant? Yes ☐ No ☐

(c) When did you last complete a PCI audit??

(d) If you outsource payment processing to a third party, are they compliant? Yes ☐ No ☐

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

Please provide full details including the maximum number of records held in one location

4. Where applicable, are you compliant with all relevant data and privacy regulations in the jurisdictions in which you operate? E.g. GDPR, PIPEDA etc. Yes ☐ No ☐

5. Do you have data retention procedures and policies in place? Yes ☐ No ☐

6. 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 ☐

Please provide further detail, plus any additional methods of protection such as tokenisation.

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

8. Do you have restricted access to sensitive data to only those requiring it and a process in place for privileged access rights? Yes ☐ No ☐

9. 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 ☐

10. Are employees regularly required to change their passwords? Yes ☐ No ☐

11. Do administrative accounts require separate credentials? Yes ☐ No ☐

12. (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? ☐

Section G: 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 application 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 (irrespective of cause) 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 application 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 application 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