Markel Cyber 360 Canada

Cyber 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 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 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: Your Details

Name of Company (Insured):	
Principal Address:	
Postal Code:	
Locations of overseas offices and subsidiaries: (please list countries)	
Website URL:	
Date of Establishment:	
Number of Employees:	

MARKEL

Business Description:

A1. Do you anticipate any major changes in your business activities in the forthcoming 12 months? ☐ Yes ☐ No

A2. Have you undergone any mergers or acquisitions in the last 12 months or have any planned in the forthcoming 12 months? ☐ Yes ☐ No

If 'Yes' to A1 or A2, please provide full details below:

A3. Are newly acquired companies required to meet certain cybersecurity standards before they are connected to the network? ☐ Yes ☐ No ☐ N/A

A4. Are separate cybersecurity and data privacy audits always part of the formal acquisition due diligence process? ☐ Yes ☐ No ☐ N/A

A5. Please detail below your gross revenue including any fees, for the past year, current year, and next year:

Date of your financial year end: Currency: USD

	Past year	Current year (estimate)	Next year (estimate)
Canada			
USA			
Rest of world			

A6. Do you have any assets, IT infrastructure, revenue, subsidiaries, or exposure in the following locations: Afghanistan, Belarus, China, Cuba, Iran, Myanmar/Burma, North Korea, Russia, Syria, Ukraine, Venezuela, Yemen? ☐ Yes ☐ No

MARKEL

Section B: People & Governance

B1.	Do you have a dedicated individual responsible for information security?	☐ Yes	☐ No
B2.	Do you have a dedicated individual responsible for data security and privacy?	☐ Yes	☐ No
B3.	Have a corporate-wide policy governing security, privacy, and acceptable use of company property for all employees and independent contractors?	☐ Yes	☐ No
B4.	Do you have a strong password policy and employees are prevented from using default, common and known compromised passwords even if it meets complexity requirements	☐ Yes	☐ No
B5.	Do you carry out employee security awareness and data security training annually?	☐ Yes	☐ No
B6.	Do you carry out phishing training for all employees?	☐ Yes	☐ No
B7.	Have you mapped and collated an up-to-date hardware and software asset inventory database?	☐ Yes	☐ No
B8.	Do you have any end-of-life or end-of-support software on your network?	☐ Yes	☐ No
B9.	Do you require vendors to demonstrate adequacy of their IT security and risk management procedures?	☐ Yes	☐ No
B10.	Do you require vendors to indemnify you contractually in respect of their data breaches and system downtime?	☐ Yes	☐ No

Section C: Access Controls

C1. Do you enforce MFA for the following:

Critical information inside the network	Remote access for all employees
Access to corporate email accounts	Remote access for all third-party contractors/vendors
Administrator and privileged accounts	Personal devices when connecting to network

C2. Have you disabled access to external Remote Desktop Protocol (RDP)? ☐ Yes ☐ No

If No, are the following implemented:

☐ VPN access only ☐ MFA ☐ RDP honeypot(s) ☐ Other

C3. Have you disabled local admin rights on workstations for standard users? ☐ Yes ☐ No

C4. Do all administrative/privileged accounts have unique credentials? ☐ Yes ☐ No

MARKEL

Section D: Network Security

D1. Do you have the following email controls in place (select all that apply):

Filtering for malicious attachments/links "Tagging" of external emails SPF DKIM

DMARC Sandboxing Phishing Reporting Tool Phishing Simulations

D2. How often do you conduct vulnerability scanning of the devices on your network?

☐ Continuously ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Yearly

☐ If other, please specify:

D3. What is your target timeframe to deploy critical patches?

☐ <24hrs ☐ 24hrs – 72hrs ☐ 3 – 7 days ☐ 7-14 days ☐ >14 days ☐ ≥30 days ☐ ≥60 days

D4. Do you use anti-virus, anti-spyware and anti-malware software? ☐ Yes ☐ No

D5. Have you configured host-based and network firewalls to disallow inbound connections? ☐ Yes ☐ No

D6. Do you use intrusion detection or intrusion prevention systems (IDS/IPS)? ☐ Yes ☐ No

D7. Have you deployed an endpoint protection platform (EPP) and/or endpoint detection and response (EDR) or MDR tool that covers 100% of:

☐ Workstations ☐ Servers ☐ EPP ☐ EDR ☐ MDR ☐ None

Which security tools do you use?

Section E: Data Risk

E1. Do you collect, process or store any of the following types of sensitive data?

	Number of records stored
☐ Basic PII (e.g. names, address, telephone numbers)	
Sensitive PII (e.g. bank account information, identity information)	
Personal health information (PHI)	
Payment card information (PCI)	
Biometrics	

E2. Do you have a data classification policy? ☐ Yes ☐ No

E3. Do you have data retention procedures and policies in place? ☐ Yes ☐ No

E4. Do you utilise encryption in the following scenarios? Select all that apply

At rest In transit Removable media Backup tapes

MARKEL

E5. Do you accept payment cards for goods or services? ☐ Yes ☐ No

If yes, are you PCI compliant? ☐ Yes ☐ No

E7. Is Credit/Debit card data encrypted or tokenized at all times? ☐ Yes ☐ No

Section F: Network Resilience

F1. How frequently do you back up critical data?

☐ Continuously ☐ Daily ☐ Weekly ☐ Monthly ☐ Other

If other, please specify:

F2. Are your backups subject to the following (select all that apply):

Segmentation Encryption MFA Vaulted or separate credentials Offline/air gapped

Immutable/read-only

F3. Do you test a full recovery from your backup? ☐ Yes ☐ No

If yes, how frequent are these tests conducted?

☐ Daily ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Other

If other, please specify: f

F4. Do you have a cyber incident response plan (IRP)? ☐ Yes ☐ No

F5. Do you have a cyber business continuity plan (BCP)? ☐ Yes ☐ No

Section G: Operational Technology (Only if applicable)

G1. Do you segregate operational technology from your information technology environment? ☐ Yes ☐ No

G2. Do you block direct internet connections to the OT network? ☐ Yes ☐ No

G3. Do you enforce MFA for 100% of remote connections to OT environment? ☐ Yes ☐ No

MARKEL

Section H: Cyber Crime

H1.	Does the applicant provide mandatory training on social engineering, phishing, to all employees that release company or client assets?	☐ Yes	☐ No
H2.	Do you have dual controls in place so that at least two people are required to process financial transactions and to disburse assets?	☐ Yes	☐ No
H3.	Prior to transferring funds to an account not previously used (new payee or changing payee accounts). Do verify the new account details with the recipient using a method of authentication distinct from the original request method?	☐ Yes	☐ No
H4	Is senior management approval always required before the change is processed, such approval being given after review of the underlying request and the record of its verification?	☐ Yes	☐ No
H5.	Is the first payment to a new supplier bank account always capped and confirmation of receipt always obtained before any further payment are made to that account?	☐ Yes	☐ No

Section I: Media Risk

I1.	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 such content?	☐ Yes	☐ No
I2.	Do you have a process in place to review media content prior to publication?	☐ Yes	☐ No
I3.	Do you have a qualified attorney to review the above?	☐ Yes	☐ No

MARKEL

Section J: Claims and Insurance History

J1.	Have you previously been insured for cyber risks?	☐ Yes	☐ No
	If yes, has the previous insurer declined, cancelled, or non-renewed coverage?	☐ Yes	☐ No
J2.	Have you terminated the contract of any IT staff members in the last 12 months due to malicious or dishonest actions?	☐ Yes	☐ No
J3.	If yes, please provide more details regarding the incident and what steps were taken after to mitigate the incident(s) in the box below.	☐ Yes	☐ No
J4.	In the last 5 years have you received or sustained, or are there currently pending, any claims, complaints, or incidents which may be covered under the proposed insurance and/or do you have knowledge of any fact, circumstance, situation, event or transaction which may give rise to a claim or loss under the proposed insurance?	☐ Yes	☐ No
J5.	If yes to any of the above please provide full details including date of loss, total dollar amount of loss, type of incident, a brief description of what occurred, and steps that were taken after the fact to mitigate the incident(s).	☐ Yes	☐ No

Section K: Declarations

I the undersigned hereby confirm that I am duly authorised and do give consent to the use of information as set out above.

I also hereby declare that I am authorized to complete this proposal on behalf of the proposer. I undertake to inform underwriters of any material alteration or addition to these statements or particulars which occurs before 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. Signing of this proposal does not bind underwriters to offer nor the applicant to accept insurance.

Any material change in Underwriters exposure must be reported prior to coverage applying.

NOTE: The signatory must be a director, senior officer, or a partner of the company.

Signature:	
Name:	
Company Position:	
Agent/Broker Contact Details:	
Date:	

MARKEL

Markel Cyber 360 Canada
Guardian 360 Pre-Breach Services

Did you know eligible policyholders can be granted access to one of the following Guardian 360 offering alongside their pre-breach onboarding call and Black Kite access; each includes a curated menu of cyber and privacy services, with policyholders able to select one preferred service. Speak to your broker for more information.

Guardian 360 Core

Breach partners may provide updates on Privacy, Cyber and AI, or an initial cyber risk consultation or contract review, including:

1. Weekly privacy updates plus quarterly Privacy, Cyber & AI roundtables with industry experts
2. High-level review of cybersecurity governance, with regulatory guidance and identification of key risks
3. Review of up to two critical contracts with insights on potential risks

Guardian 360 Plus

Breach partners may provide cyber risk assessments, tabletop exercises or contract reviews, including:

1. Assessment or development of an incident response plan, with identification of regulatory gaps
2. A virtual one-hour tabletop exercise with key stakeholders
3. Customized checklist mapping relevant federal and provincial cyber regulations
4. Review of up to five critical contracts with insights on potential risks

Guardian 360 Pro

Breach partners may offer policy or contract reviews, tabletop exercises, and regulatory checklists, including:

1. Review of up to two key policies, with expert recommendations for compliance and best practices
2. A tailored two-hour tabletop exercise followed by a debrief to strengthen preparedness.
3. Customized checklist outlining applicable federal and provincial cyber regulations
4. Review of up to five critical contracts, offering insight into potential risks and recommended clause enhancements to support compliance and resilience

Guardian 360 Ultra

Breach partners may provide a full cyber readiness assessment, incident response plan drafting, custom tabletop exercises, regulatory gap analyses, board/executive training or vendor management consultancy, as detailed below:

1. Full review of cyber policies, procedures, and contracts, with stakeholder interviews to assess preparedness
2. A three-hour immersive tabletop exercise with real-time feedback, followed by key takeaways and an action plan
3. A regulatory compliance review: expert gap analysis of your alignment with applicable cyber laws and regulations
4. Customized cyber risk training for executives and boards, covering legal obligations and real-world case studies
5. Vendor management guidance with risk assessment templates and standard cyber contract clauses for ongoing resilience.