Markel Cyber 360

New business application 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 . 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:	

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 your turnover, including fees, for the past year, and estimated turnover for the current and next year:

Date of your financial year end: Currency: CAD

	Past Year	Current Year (estimate)	Next Year (estimate)
Canada			
USA			
Europe			
UK			
ROW			
TOTAL			
Profit or (loss)			

MARKEL

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

---

Section B: People & Governance

B1. Annual IT Budget: _____ Percentage of IT budget spent on cyber security: _____ %

B2. Full time IT employees: _____ Full time cyber security employees: _____

B3. Do you have a dedicated information security lead (CISO, CIO, or equivalent)? ☐ Yes ☐ No

B4. Do you have a dedicated data security and privacy lead (CPO, DPO, or equivalent)? ☐ Yes ☐ No

B5. Is there a corporate-wide policy governing security, privacy, and the acceptable use of company systems and property for all employees and independent contractors? ☐ Yes ☐ No

B6. Are background checks performed on all employees and contractors with access to sensitive data or whose work involves critical IT infrastructure? ☐ Yes ☐ No

B7. Are processes in place to delete systems access within 48 hours after employee termination? ☐ Yes ☐ No

B8. Are employees prohibited from using personal email accounts on organizational systems? ☐ Yes ☐ No

B9. Do you have a strong password policy that prevents the use of default, common, or known compromised passwords? ☐ Yes ☐ No

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

B10. Please confirm which cybersecurity or data protection standards, frameworks, or best practices have been adopted and if accreditation has been obtained:

☐ ISO27001 ☐ NIST ☐ CIS ☐ PCI DSS ☐ HIPAA ☐ Other _____

B11. Do you carry out employee security awareness and data security training annually? ☐ Yes ☐ No

B12. Do you carry out phishing training for all employees? ☐ Yes ☐ No

B13. Have you mapped and collated an up-to-date hardware and software asset inventory? ☐ Yes ☐ No

B14. Do system configuration management tools enforce and redeploy settings to systems? ☐ Yes ☐ No

MARKEL

B15. Do you have a policy and process to decommission unused systems and software? ☐ Yes ☐ No

B16. Do you have any end-of-life or end-of-support software on your network? ☐ Yes ☐ No

If 'Yes', what percentage (%) of the software is end-of-life or end-of-support that supports vital systems or holds sensitive information? ____ %

If 'Yes', do you mitigate the software with:

Purchase of additional support | Increased altering/monitoring | Additional access controls

Segmentation | None of the above

Section C: Access Controls

C1. Do you enforce MFA for the following:

Critical information inside the network | Remote access for 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 controls 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

C5. Do you utilize a Privileged Admin Management (PAM) tool? ☐ Yes ☐ No

---

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. What percentage (%) of your enterprise is covered by scheduled vulnerability scans? ____ %

D3. How often do you conduct vulnerability scanning of the devices on your network?

☐ Continuously ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Yearly

☐ If other, please specify: _____

MARKEL

D4. What is your target timeframe to deploy critical patches?

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

D5. Do you use anti-virus, anti-spyware and anti-malware software? ☐ Yes ☐ No

D6. Have you configured host-based and network firewalls to disallow inbound connections? ☐ Yes ☐ No

D7. Do you use intrusion detection or intrusion prevention systems (IDS/IPS)? ☐ Yes ☐ No

D8. 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 tool(s) do you use?

D9. Do you operate a 24/7 SOC? ☐ Yes ☐ No

D10. Do you operate a SIEM tool? ☐ Yes ☐ No

D11. Does the SIEM feed into the SOC? ☐ Yes ☐ No

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. Please estimate the maximum number of unique records held within your single largest repository.

E3. Are you compliant with all relevant data and privacy regulations in the jurisdictions in which you operate? ☐ Yes ☐ No

E4. Do you isolate critical/sensitive information in its own segregated environment? ☐ Yes ☐ No

E5. Do you have a data classification policy? ☐ Yes ☐ No

E6. Do you have data retention procedures and policies in place? ☐ Yes ☐ No

MARKEL

E7. Do you utilize encryption in the following scenarios? Select all that apply:

At rest In transit Removable media Backup tapes

E8. Do you have restricted access to sensitive data to only those requiring it and a process in place for privileged access rights? ☐ Yes ☐ No

If yes, is this access reconsidered at least annually? ☐ Yes ☐ No

E9. Do you accept payment by card for goods or services? ☐ Yes ☐ No

If yes, are you compliant with PCI DSS security standards? ☐ Yes ☐ No

E10. What level of PCI Merchant are you?

E11. Is credit and debit card data encrypted or tokenized at all times? ☐ Yes ☐ No

E12. Do you outsource all transactions through a payment processor? ☐ Yes ☐ No

If so, are they PCI DSS compliant? ☐ Yes ☐ No

E13. Is your POS network segregated from the rest of the corporate environment? ☐ Yes ☐ No ☐ N/A

Section F: Network Resilience

F1. Do you segment your network based on any of the criteria below? Select all that apply:

By geography System criticality/sensitivity Business function

F2. How frequently do you back up critical data?

☐ Continuously ☐ Daily ☐ Weekly ☐ Monthly ☐ Other

If other, please specify:

F3. Are your backups subject to the following (select all that apply):

Segmentation Encryption MFA Vaulted or separate credentials Immutable/read-only

Offline/air gapped

F4. 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 yes, please specify:

MARKEL

F5. Do you test the integrity of backups prior to restoration to be confident they are free from malware? ☐ Yes ☐ No

F6. How long would it take to restore all of your critical data from back-ups?

☐ <48hrs ☐ <7 days ☐ >7 days ☐ Unknown

				Date of last test:
F7.	Do you have an incident response plan (IRP)?	☐ Yes	☐ No	
F8.	Do you have a disaster recovery plan (DRP)?	☐ Yes	☐ No	
F9.	Do you have a business continuity plan (BCP)?	☐ Yes	☐ No	
F10.	Does your incident response plan (IRP) specifically address ransomware scenarios?	☐ Yes	☐ No	

Section G: Vendor Management

G1. Do you require vendors to demonstrate adequacy of their IT security and risk management procedures? ☐ Yes ☐ No

G2. Do you require contractors to undergo security awareness and data security training? ☐ Yes ☐ No

G3. Do you require vendors that supply critical services or hold personal information to procure and evidence E&O and Cyber insurance for the services they provide to you? ☐ Yes ☐ No

G4. Do you require vendors to indemnify you contractually in respect of their data breaches and system downtime? ☐ Yes ☐ No

Section H: Operational Technology (Only if applicable)

H1. Do you have a dedicated person responsible for OT security? ☐ Yes ☐ No

H2. Do you maintain up to date inventory of all IT and OT assets? ☐ Yes ☐ No

H3. Do you segregate operational technology from your information technology environment? ☐ Yes ☐ No

H4. Do you block direct internet connections to the OT network? ☐ Yes ☐ No

H5. Do you enforce MFA for 100% of remote connections to OT environment? ☐ Yes ☐ No

H6. Does segmentation exist between each of your sites and production lines? ☐ Yes ☐ No

MARKEL

Section I: Cyber Crime

I1.	Does the applicant provide mandatory training on social engineering, phishing, to all employees that release company or client assets?	☐ Yes	☐ No
I2.	Do you have dual controls in place so that at least two people are required to process financial transactions and to disburse assets >$25,000?	☐ Yes	☐ No
I3.	Prior to transferring funds to an account not previously used (new payee or changing payee accounts). Do you verify the new account details with the recipient using a method of authentication distinct from the original request method?	☐ Yes	☐ No
	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
I4.	Is the first payment to a new supplier bank account always capped and confirmation of receipt always obtained before any further payments are made to that account?	☐ Yes	☐ No

Section J: Media Risk

J1.	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
	If yes, does the content include streaming video and music?	☐ Yes	☐ No
J2.	Do you allow third parties to post content directly to the website?	☐ Yes	☐ No
J3.	Do you monitor content for offensive, harassing, infringing or other undesirable material?	☐ Yes	☐ No
	If so, do you reserve the right to remove or censor any content that violates the acceptable terms of use?	☐ Yes	☐ No
J4.	Do you have formal, written policies and procedures for addressing requests to remove allegedly offensive or infringing content disseminated by or on behalf of you?	☐ Yes	☐ No
J5.	Do you have a process in place to review media content for the following prior to publication:		
	Infringement of copyright	☐ Yes	☐ No
	Infringement of trademark	☐ Yes	☐ No
	Libel/slander	☐ Yes	☐ No
	Invasion of privacy	☐ Yes	☐ No
J6.	Do you have a qualified attorney to review the above?	☐ Yes	☐ No

MARKEL

Section K: Claims and Insurance History

K1. Have you previously been insured for cyber risks? ☐ Yes ☐ No

K2. Has any insurance policy providing substantially the same or similar insurance as the insurance being applied for under this application been declined, cancelled or non-renewed at the choice of the insurer? ☐ Yes ☐ No

K3. Have you terminated the contract of any IT staff members in the last 12 months due to malicious or dishonest actions? ☐ Yes ☐ No

K4. 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

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

Section L: Declarations

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

I also hereby declare that I am authorized to complete this application on behalf of the applicant. 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 the applicant's exposure must be reported prior to coverage taking effect.

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.