Cyber Insurance

A comprehensive cyber and data risks solution

Proposal form

Important notice

1. This is a proposal for a contract of insurance, in which 'proposer' or 'you/your' means the individual, company, partnership, trust, charity, establishment or association proposing for cover.
2. This proposal form 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 Underwriters to enter into any contract of insurance. If space is insufficient to answer any question fully, please attach a signed continuation sheet. You should retain a copy of the completed proposal (and of any other supporting documentation) for future reference.
3. You are recommended to request a specimen copy of the proposed policy or certificate from your insurance broker and to consider carefully the terms, conditions, limitations and exclusions applicable to the cover. The proposed insurance covers only those losses which arise from certain events discovered or claims made against the Assured during the period of insurance, as specified in the policy or certificate.

Your Details

Proposer

Full name/Trading name			
Subsidiary Companies to be covered under this policy			
Correspondence Address (street address, postcode)			
Web address			
Contact Email Address			
Industry Sector		No. of Employees	
Full Description of Business Activities			

MARKEL

1. **Please provide your total turnover for the last 12 months, split by territory:**

UK	EEA	USA/Canada	ROW
£	£	£	£

2. **What percentage of your turnover is from online/internet sales?** %

3. **Do you have access to any NHS systems or networks?** ☐ Yes ☐ No

4. **Please provide an estimated total number of Personally Identifiable Information (PII) records held at any one time.**

(a) Of this number, how many records would be considered sensitive?

For example, health/medical records, passport numbers, social security numbers, payment card/financial information, biometric data.

5. **Select all the following that apply to any proposer/director/partner of the business/practice:**

Previous lawsuit for infringement of privacy	☐ Yes	☐ No
Previously sustained any unscheduled or unintentional network outage	☐ Yes	☐ No
Previously declared bankrupt, insolvent or gone into liquidation or have outstanding CCJ's	☐ Yes	☐ No
Previous conviction(s) of a criminal offence other than a motoring offence	☐ Yes	☐ No
Insurance previously declined/renewal refused/special terms imposed	☐ Yes	☐ No
Offices outside the UK	☐ Yes	☐ No

If yes to any statements in **5**. please provide full details.

6. **In the last five years has the Proposer suffered a loss or claim under a cyber policy or experienced any cyber or privacy incidents?** ☐ Yes ☐ No

If yes, please provide further details.

Date of claim/incident	Total Paid	Is claim/incident settled?	Reserve Amount
	£		£
	£		£
	£		£
	£		£
	£		£
	£		£

MARKEL

Please describe the claim/incident circumstances, and what steps have been taken to prevent a reoccurrence:

Your Controls

7. **Do all employees use Multi-factor Authentication (MFA) when accessing your computer network remotely?** ☐ Yes ☐ No

8. **How frequently do you back up your critical data?**

☐ Daily ☐ Weekly ☐ Monthy ☐ Quarterly

9. **Do you have a process in place to verify any changes or additions of bank account details for all account payments with a known client contact, prior to actioning?** ☐ Yes ☐ No

Supplementary Questions

(for businesses £50m+ in turnover, or when requested by an underwriter)

10. **Is your organisation currently accredited with any of the following?**

☐ Cyber Essentials ☐ Cyber Essentials Plus ☐ ISO/IEC 27001 ☐ Other (please state below)

11. **Do you have Multi-factor Authentication (MFA) in place to access:**

☐ Cloud-based services and applications ☐ Internal administrative access ☐ Email and webmail

12. **Do you keep a copy of backups:**

☐ Offline ☐ Offsite ☐ Immutable ☐ Isolated from your live environment
☐ Protected with MFA

13. **Do you authenticate emails using:**

☐ SPF (Sender Policy Framework)
☐ DomainKeys Identified Mail (DKIM)
☐ Domain-based Message Authentication, Reporting and Conformance (DMARC)

MARKEL

14. Do you utilise an Endpoint Detection and Response (EDR) product? ☐ Yes ☐ No

a. Which EDR provider do you use? _____

b. What percentage of your network is covered by EDR? _____ %

15. Is access to your Remote Desktop Protocol (RDP) protected with:

☐ VPN ☐ MFA ☐ A strong password policy

16. How do you segment your network?

☐ By location ☐ By business function ☐ By sensitivity of data

17. What PCI DSS Merchant Level do you follow?

☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4

18. Do you provide cyber security training to your employees

☐ Ad-hoc ☐ On induction ☐ Annually

19. Do you carry out phishing simulations? ☐ Yes ☐ No

a. Do you follow up on failed phishing simulations with additional training? ☐ Yes ☐ No

20. Do administrative/privilege accounts use a Privilege Access Management (PAM) tool? ☐ Yes ☐ No

21. What is the estimated time taken to install security patches across your network?

☐ 0-7 days ☐ 7-14 days ☐ 14-30 days ☐ 30+ days

22. Do you have the ability to fast-track patch installation to prevent zero-day exploitations? ☐ Yes ☐ No

23. Do you operate an SIEM (Security Information and Event Management?) ☐ Yes ☐ No

a. Is your SIEM monitored 24/7/365 by:

☐ An internal SOC (Security Operations Centre)

☐ An external SOC or MSSP (Managed Security Service Provider)

24. Do you use any software that is end of life, legacy or no longer supported by the developer? ☐ Yes ☐ No

a. If yes, is the software:

☐ Connected/exposed to the internet

☐ Exposed to, or hosting, any critical or sensitive data

☐ Segmented by firewalls or VLAN

b. Have you purchased any extended support? ☐ Yes ☐ No

MARKEL

25. Do you encrypt sensitive data:

☐ At rest ☐ In transit ☐ On portable media devices

26. Do you have antivirus and firewalls in place? ☐ Yes ☐ No

a. What type of firewalls do you use? e.g. next-generation, perimeter.

b. Can ordinary users change firewall rules or disable antivirus? ☐ Yes ☐ No

27. Do you test successful restoration of your backups? ☐ Yes ☐ No

a. If yes, how often?

28. Do you have in place:

☐ A business continuity plan (BCP) ☐ A disaster recovery plan (DRP)

a. Does your BCP/DRP include response to a cyber incident, including ransomware? ☐ Yes ☐ No

b. Do you carry out a tabletop exercise of your BCP/DRP at least annually? ☐ Yes ☐ No

29. How often do you carry out vulnerability scanning across your network?

☐ Daily ☐ Weekly ☐ Monthy ☐ Quarterly

a. What percentage of your network is covered by your scans? %

30. Do you carry out penetration testing at least annually? ☐ Yes ☐ No

31. Do you utilise any Operational Technology (OT) in your business processes?
For example, SCADA, CNC, HVAC systems. ☐ Yes ☐ No

a. How is your OT network secured?

☐ Segmented from your IT network

☐ Disconnected from the internet

☐ MFA in place for remote access

32. Do you rely on any cloud-based services? ☐ Yes ☐ No

a. If yes, please provide the names of the top 3 providers and what services they supply you with:

Name of provider	Function

MARKEL

33. Can you confirm there is strict compliance to dual controls in place, ensuring at least two people are required for the following:

a.	Appointing new suppliers or awarding contracts	☐ Yes	☐ No
b.	Opening and amending bank accounts/mandates	☐ Yes	☐ No
c.	Processing financial transactions including depositing or withdrawing of funds	☐ Yes	☐ No

Declaration

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 authorised 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.

*Signed:	Name:
Agent/Broker contact details:	
Company position:	Date:

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