



## Cyber Liability Insurance Questionnaire

**1. Company Name**

---

**2. NAICS / Industry Code or Description**

**3. Year Business Established**

---

---

**4. Street Address**

**5. City, State, Zip**

---

---

**6. Current Revenue**  
(Most Recent Fiscal Year)

**7. Projected Revenue**  
(Next Fiscal Year)

**8. Number of Employees**

---

---

---

**9. Does the company have any revenue-generating operations outside of the US?**

Yes

No

**10. Any merger/acquisition/divestment or bankruptcy proceeding/financial restructuring in the past 12 months or next 12 months?**

Yes

No

**9 (a). If yes, what percentage is outside the US?**

**11. Entity Type**

**12. Ownership Type**

**13. Domain Names**

Holding

Non-Profit

Independent

Private

Parent

Public

Subsidiary

Public Sector

Partnership

**14. Desired Limits**

**15. Policy Deductible**

**16. Proposed Effective Date**

---

---

---

17. Do policyholder employees authenticate fund transfer requests, prevent unauthorized employees from initiating wire transfers, verify vendor/supplier bank accounts before adding them to accounts payable systems, and complete annual anti-fraud training? Yes  
No
18. Does the policyholder provide mandatory security training to all employees annually and ensure third-party service providers comply with IT standards? Yes  
No
19. For sensitive information stored on the cloud, does the policyholder encrypt all emails, mobile, and computing devices sent to external parties? Yes  
No
20. Does the policyholder enforce Multi-Factor Authentication (MFA) for all employees, contractors, and partners, in addition to cloud deployments, email, mission-critical systems, privileged accounts, VPN, and remote access? Yes  
No
21. In the last five (5) years, have you or any other proposed insured know of any past, current, or pending fact, circumstance, situation, event, or transaction surrounding cyber incidents, extortion demands, civil/criminal actions, administrative proceedings, media liability/intellectual property complaints or claims, including any incidents that did or did not require notification under state or federal regulations, or resulted in loss of business income due to unscheduled system downtime? Yes  
No
22. Does the policyholder collect, host, store, control, use, process, share, transmit, or have access to any PCI, PII, PHI, or biometric data? If yes, answer the two questions below: Yes  
No
- 22 (a). How many PII and PHI records does the policyholder collect, process, store, transmit, or have access to?
- 22 (b). What is the estimated volume of payment card transactions (credit cards, debit cards, etc.)?
23. Does the policyholder protect all devices with encryption, anti-virus, anti-malware, and/or endpoint protection software along with pre-screening emails for potentially malicious attachments and links? Yes  
No

24. Does the policyholder maintain at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network? Yes  
No
25. Does the policyholder have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to publication, broadcast, distribution, or use? Yes  
No

Signature: \_\_\_\_\_

Date: \_\_\_\_\_