

CYBER LIABILITY SUPPLEMENTAL APPLICATION

SECTION I – INTRODUCTION

1. Full Name of Applicant:
(Include all prior names, DBAs and subsidiaries seeking coverage under the policy for which you are applying)

2. Website Address(es):

3. Have you experienced any mergers, acquisitions, or divestitures in the last 5 years? Yes No
 Do you plan on any within the next 12 months? Yes No
 If Yes to either of the above, provide complete details:

SECTION II - NETWORK SECURITY & DATA PRIVACY

PART 1 – INTERNAL TRAINING, POLICIES AND PROCEDURES

4. Do you conduct employee training on an annual basis (or more frequently) related to:

a. HIPAA Compliance	Yes	No
b. Company Incident Reporting Procedures	Yes	No
c. Document Management	Yes	No
d. Internet and Email Use	Yes	No
e. Passwords	Yes	No
f. Responsibility for Company Data	Yes	No

5. Do you conduct cyber competency testing on an annual basis (or more frequently) for employees and contractors on:

a. Social engineering attacks (i.e. email-based phishing, baiting, scareware, etc.)	Yes	No
b. Physical security (locked and secured computer devices)	Yes	No

6. Do you use any of the following technology:

a. Meta Pixel or similar technology on your website	Yes	No
b. Session Replay or similar technology	Yes	No
c. Chatbot or similar technology	Yes	No

If Yes to any of the above, do you request affirmative consent from users? Yes No
 If No, describe below:

7. Do you have rapid (immediate) account access termination procedures for employees that leave the company? Yes No
8. Do you have a privacy policy? Yes No
 If Yes, has it been reviewed by legal representation? Yes No
9. Do you maintain an incident response plan which includes business continuity mitigation procedures in the event of a ransomware threat? Yes No

10. a. Are you compliant with the following:

	Indicate N/A, Yes or No			Date of Last Audit/Assessment
Health Information Portability and Accountability Act (HIPAA)	N/A	Yes	No	
Health Information Technology for Economic and Clinical Health Act (HITECH)	N/A	Yes	No	
Payment Card Industry Data Security Standards (PCI DSS)	N/A	Yes	No	

b. If you are subject to PCI DSS, what is your certification level?

c. Complete the chart below for any of the following assessments you have completed:

	Indicate N/A, Yes or No			Date of Last Audit/Assessment
SOC II Certification Type I	N/A	Yes	No	
SOC II Certification Type II	N/A	Yes	No	
Biometric Information Privacy Act (BIPA)	N/A	Yes	No	

d. Describe any changes made to operations, procedures and/or network security and data privacy practices as a result of the recent Audits/Assessments listed in the two charts above:

PART 2 – NETWORK SECURITY AND DATA PRIVACY CONTROLS

11. a. Where do your servers reside? Cloud On Premises
- b. If cloud, which vendor(s) do you use?
- c. Are your production servers separated in different locations? Yes No
12. a. Is your network managed in-house or by a vendor?
- b. If outsourced, which vendor(s) do you use?
- c. What are the qualifications of your IT security leaders? (Examples: CISSP, CISM, CISA, CEH, CCSP)

13. Indicate all IT risk management elements implemented:

	In-House	Vendor		In-House	Vendor
Access Restrictions			Hot Site		
Anti-Virus Scanning			Load Balancers		
Automated Security Scanning			Proxy Servers		
Network Intrusion Detection			Security Audits		
Encryption			Secure Remote Capabilities		
Firewall			Other:		

14. What types of network monitoring solutions (active and passive) do you have in place, and who does the monitoring?

15. How frequently do you test your network security to ensure effectiveness and response time?

Monthly Quarterly Annually

16. What are your procedures for correcting vulnerabilities from penetration testing?

17. a. How often do you patch:

Server infrastructure:

Desktop/laptop infrastructure:

b. If you are a software company, how often do you issue patches?

c. Are you responsible for patching any systems for customers?

Yes No

If Yes, how frequently?

d. How do you respond to Zero-Day vulnerabilities? *(A Zero-Day vulnerability or exploit is a vulnerability that has been disclosed but not yet patched. Recent example: log4j.)*

18. Do you employ Endpoint Detection and Response (EDR) security tools?

Yes No

19. Do you employ network segmentation to separate critical systems, applications, and data from non-critical?

Yes No

20. Do you employ Multi-Factor Authentication for the following:

a. Critical Information

Yes No

b. Remote Access

Yes No

c. Administrator and privileged user accounts

Yes No

d. Personal devices accessing the network

Yes No

e. Independent contractor and vendors accessing the network

Yes No

f. Non-critical information and applications

Yes No

21. Are workstations prohibited from local admin rights?

Yes No

a. If Yes, all the time or case by case?

b. Do you manage privileged accounts using tooling such as CyberArk or other?

Yes No

c. How many users have persistent privileged accounts for endpoints (defined as those who have entitlements to configure, manage, and support endpoints)?

Describe compensating security controls for these specific persistent privileged accounts:

22. Do you route all outbound web requests through a web proxy which monitors for and blocks potentially malicious content?

Yes No

23. Are external emails tagged as such to alert your employees that the email originated from outside of your organization? Yes No
24. Do you utilize Microsoft Office 365? Yes No
- If Yes, does this include Office 365 Threat Protection add-on? Yes No
- If No, or if you use an alternate product to MS Office 365, provide details or an explanation as to why this measure has not been implemented:

25. Provide the estimated record count of sensitive information you maintain on your servers, store with a cloud provider and host for others:

	Number of Records
Medical Records	
Financial Records (credit/debit cards, bank account #'s, etc.)	
Other Protected Personally Identifiable Information (SSN's, Driver's License #, etc.)	
Biometric Information	
Protected Personally Identifiable Information of Minors	
TOTAL RECORD COUNT	

26. Do you require encryption for the following:
- a. Sensitive information while in transit? Yes No
- b. Sensitive information while at rest? Yes No
- c. Remote Access Yes No
- d. How are your encryption keys protected?

27. a. How often do you purge data?
- b. Check the following safeguards that you use for data destruction:
- Physical Destruction – Certification from vendor for physical shredding of media.
- Overwriting – Single or multiple overwriting passes with fixed pattern such as binary zeroes.
- Degaussing – Strong magnetic field applied to magnetic media to randomize field orientation.

28. How do you ensure sensitive data destruction compliance with applicable privacy law?

29. What are your data security vetting procedures for third parties that you either share data or network access to?

30. Do you use any physical security controls to prevent unauthorized access to networks and data? (Examples: controlled swipe card access with logging, security cameras, etc.) Yes No
- If Yes, describe such controls:

PART 3 – BACKUP AND RECOVERY

31. a. How often are network backups performed?
- b. How often are these backups tested?
- c. Are the backups stored offsite? Yes No
- d. Are backup files encrypted? Yes No
32. Is backup access subject to separate authorization credentials which are maintained separately from common system credentials? Yes No
33. Do you test the successful restoration and recovery of key server configurations and data from backups? Yes No
- If Yes, how often?
34. a. How often is your disaster recovery plan tested?
- b. What is your recovery time objective? (This is the time it takes to recover from an event.)
- c. What is your recovery point objective? (*This is the point in time to which you are restoring or how far back in time prior to an event that the last known backup or last known good configuration is known to exist.*)

PART 4 – CYBER CRIME

35. Is dual authorization required for all wire transfers? Yes No
- If Yes, describe authorization process including which employees or departments have the authority to do so:
36. Are transfer verifications sent to an employee or department other than the one that initiated the transfer? Yes No
37. For employees responsible for wire transfers, is training conducted regarding common wire transfer fraud attack vectors (i.e. social engineering phishing, spear phishing, whaling)? Yes No
- If Yes, how often?
38. Do you call to verify or have another verification process if a client or vendor makes a request via email to change bank account information or key information for future invoices? Yes No
- If Yes, describe:

SECTION III – CLAIMS HISTORY

39. Is the applicant aware of any errors, omissions, circumstances, or incidents which may result in a claim being made against them or their employees, or are there any claims that have not yet been reported? Yes No
- If Yes, provide complete details:

40. After inquiry, is the applicant, any predecessors in business, or any other person for whom coverage is requested aware of any act, error, omission or circumstance which may possibly result in a claim being made against them?
If Yes, provide details: Yes No
41. In the past five (5) years:
- a. Have you experienced any:
 - i. Known intrusions (i.e. unauthorized access), security incidents, security breaches or cyber-attacks? Yes No
 - ii. Actual or attempted extortion demand with respect to your computer systems? Yes No
 - iii. Unexpected outage of a computer network, application, or system lasting greater than four (4) hours? Yes No
 - b. Have you experienced an actual or suspected data breach or cyber-attack?
If Yes, provide a detailed description of the event(s) and remediation action(s) taken: Yes No
 - c. Have you received any complaints concerning the content of your websites or electronic communications?
If Yes, provide complete details: Yes No
 - d. Have you been accused of, made aware of, or had a claim as a result of actual or alleged infringement upon another's domain name, trademark, copyright, services mark or similar intellectual property?
If Yes, provide complete details: Yes No

If yes, complete the [Supplemental Claim Information Form](#) for each and every claim.

Fraud Notices

Applicable in AL, AR, DC, LA, MD, NM, RI and WV: Any person who knowingly (or willfully)* presents a false or fraudulent claim for payment of a loss or benefit or knowingly (or willfully)* presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison. *Applies in MD only.

Applicable in CO: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

Applicable in FL and OK: Any person who knowingly and with intent to injure, defraud or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony (of the third degree)*. * Applies in FL only.

Applicable in KS: Any person who knowingly and with intent to defraud, presents, causes to be presented, or prepares with knowledge or belief that it will be presented, to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act.

Applicable in KY, NY, OH and PA: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties (not to exceed five thousand dollars and the stated value of the claim for each such violation)*. *Applies in NY only.

Applicable in ME, TN, VA, and WA: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties (may)* include imprisonment, fines and denial of insurance benefits. *Applies in ME only.

Applicable in NJ: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Applicable in OR: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact may be violating state law.

Applicable in PR: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation by a fine of not less than five thousand dollars (\$5,000) and not more than ten thousand dollars (\$10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances [be] present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Applicable in all other States: Any person who knowingly and with intent to defraud any insurance company or other person, files an application for insurance, or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any material fact, commits a fraudulent insurance act, which is a crime and may also be subject to civil penalty.

Other State Notices

Applicable in RI: THIS INSURANCE CONTRACT HAS BEEN PLACED WITH AN INSURER NOT LICENSED TO DO BUSINESS IN THE STATE OF RHODE ISLAND BUT APPROVED AS A SURPLUS LINES INSURER. THE INSURER IS NOT A MEMBER OF THE RHODE ISLAND INSURERS INSOLVENCY FUND. SHOULD THE INSURER BECOME INSOLVENT, THE PROTECTION AND BENEFITS OF THE RHODE ISLAND INSURERS INSOLVENCY FUND ARE NOT AVAILABLE.

I/We understand that this is an application for insurance only and that the completion and submission of this Application does not bind the Company to sell nor the applicant to purchase this insurance. I/We hereby declare that the above statements and particulars are true and I/we agree that this Application shall be the basis for any contract of insurance issued by the Company in response to it.

Electronic Signature of Applicant or Authorized Representative:

Title:

Date:

If you prefer not to return the questionnaire with an electronic signature, please print and sign.