



GREAT AMERICAN ASSURANCE COMPANY
Professional Liability - Supplemental
Cyber Loss & Liability Application

Firm Name: _____

Name & contact information of person responsible for IT security: _____

Email address: _____ Firm's Website: _____

1. Does the applicant currently purchase any form of cyber risk insurance on either a stand-alone basis or by endorsement to any policy? Yes No
If "Yes", please provide a copy of the current policy's Declarations.

2. After inquiry is the applicant, or anyone to whom this Insurance applies, aware of any:
- a. acts, errors or omissions which you have reason to believe could give rise to a cyber related claim? Yes No
 - b. intrusion, malware or other IT security related event in the last five (5) years that resulted in you incurring legal, forensic or other related expenses? Yes No

If Yes to any of the above, please detail in a separate attachment a description of the incident including relevant dates, the number and type of records involved, the total dollar amount of expenses in connection with the incident, a summary of the Company's response to the security breach, and subsequent changes made to prevent the likelihood of future events.

NOTE: IT IS AGREED THAT ANY CLAIM, LOSS OR COSTS ARISING FROM ANY FACT, CIRCUMSTANCE, SITUATION, TRANSACTION, EVENT, ACT, ERROR OR OMISSION REQUIRED TO BE DISCLOSED IN RESPONSE TO QUESTION 2 IS EXCLUDED FROM COVERAGE.

3. Please estimate the annual volume of each type of information you process or store, taking into account both electronic and paper files as well as employee AND customer information:
- a. SSN, individual taxpayer I.D., driver's license, passport, or federal ID numbers: _____
 - b. payment card data (credit or debit card): _____
 - c. protected health information: _____
 - d. other confidential or protected information: _____

4. a. Do you have a record retention/destruction policy in place? Yes No
b. How long do you store records? _____ years

5. Your policy regarding the encryption of confidential data (including but not limited to client financials and/or personally identifiable information referenced above) is that such data should be encrypted:
- never/you don't encrypt
 - within your network only
 - within your network and on portable devices (i.e. laptops and smartphones)
 - within your network, on portable devices and on all removable/transportable storage media (USB drives, discs, etc.)

6. The applicant backs up its critical systems & data assets:
- a. daily/nightly weekly or biweekly less frequently than biweekly
 - b. is the backup system remote and secure? Yes No
 - c. are the backup procedures tested at least annually? Yes No

7. Does the applicant publish any original works (books, journals, white papers, etc.) as part of its business? Yes No

8. Does the applicant have an established procedure for editing or removing content that might be construed as libelous, slanderous, or infringing on the intellectual property rights of others? Yes No

9. Does the applicant provide any of the following to its clients:
 software support IT consulting apps none of these (n/a)
10. Please indicate which of the following are part of the Company's privacy and network security programs
(select all that apply):
- a. physical controls on access to computer systems and sensitive documents
 - b. password protection on company devices
 - c. multi-factor authentication for remote access to e-mail and both internal and external systems
 - d. up-to-date, active firewall & anti-virus software
 - e. an email filtering solution
 - f. phishing training
 - g. advanced endpoint detection, protection and response
 - h. 24/7/365 endpoint security monitoring
 - i. "principle of least privilege" (i.e. bare minimum privileges necessary to perform job function) applied to all roles
11. Indicate which of the following controls you have implemented with respect to electronic fund transfers:
- a. callback procedures to verify fund transfer requests or changes to banking information
 - b. dual authorization for fund transfers
 - c. not applicable, we do not perform any electronic fund transfers
12. The Company's policy is to push general patches within 30 days and critical patches within 14 days. Yes No
13. The Company has a process in place to monitor and respond to zero-day vulnerabilities (i.e. a vulnerability in a system or device that has been disclosed but is not yet patched) within 5 days or less. Yes No
14. The Company maintains Business Continuity Plans and Incident Response Plans to address network security incidents including ransomware and data breaches. Yes No
15. The Business Continuity Plans and Incident Response Plans are tested at least annually. Yes No

FRAUD WARNING: 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.

I understand that the information submitted in this supplement becomes a part of my Professional Liability Errors & Omissions application and is subject to the same representations and conditions.

 Print Name

 Title

 Signature

 Date

Florida, Iowa and New Hampshire Agents Only, please provide the following: License # _____

Producer name _____ Signature: _____