



301 E. Fourth Street, Cincinnati, OH 45202

Application
For
Cyber Risk Insurance Policy

INSURING AGREEMENT I.B. OF THIS POLICY IS WRITTEN ON A CLAIMS MADE BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD. COSTS OF DEFENSE REDUCE AND MAY EXHAUST THE APPLICABLE LIMIT(S) OF LIABILITY AVAILABLE TO PAY SETTLEMENTS, JUDGMENTS OR OTHER COSTS. LOSS, INCLUDING COSTS OF DEFENSE AND OTHER COVERED COSTS ARE SUBJECT TO THE APPLICABLE RETENTION. PLEASE READ THE POLICY CAREFULLY. COMPLETION OF THIS APPLICATION IN NO WAY WILL BE CONSIDERED A BINDER OF COVERAGE.

Part I - GENERAL INFORMATION

Company Name:
Street Address:
City, State, Zip:

Person responsible for buying coverage: Email:

Year the Company was established:

Total revenues most recent fiscal year: \$

Projected revenue for the current fiscal year: \$

Total number of locations:

Total number of employees:

Description of operations:

SIC code(s):

List of Subsidiaries of the Company:

List of Websites:

Part II - COVERAGE INFORMATION

Prior Coverage

- 1. Does the Company currently purchase any form of Privacy, Cyber, or Network Liability insurance...
2. Has the Company ever been declined coverage for Privacy, Cyber, Network, or Media Liability...
3. Has the Company ever experienced any claims that would be covered by this policy...

Prior Breaches/Losses

4. Has the Company or any Subsidiary had any of the following situations occur in the past five years (internal or external origination)?

- a) Loss or theft of data?
b) Unscheduled systems outage?
c) Data breach requiring the Company to notify individuals of the breach?
d) Loss of any laptop, smartphone, or other mobile device?
e) A systems intrusion, tampering, virus or malicious code attack, hacking incident?
f) A dispute with a third-party over content that was used?
g) Regulatory inquiry, investigation or action?
h) Allegations by anyone (including allegations by employees of the Company) that their personal information has been compromised?
i) Loss of business income as a result of a security breach?

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

NOTE: IT IS AGREED THAT ANY CLAIM, BREACH OR LOSS REQUIRED TO BE DISCLOSED IN RESPONSE TO THIS QUESTION IS EXCLUDED FROM THE PROPOSED INSURANCE, AND 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 THIS QUESTION IS EXCLUDED FROM COVERAGE.

5. Is the undersigned aware of any fact, circumstance, situation, transaction, event, act, error or omission involving the Company or any of its Subsidiaries which the undersigned has reason to believe may or could reasonably be foreseen to give rise to a claim or loss that may fall within the scope of the proposed insurance?

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 5. IS EXCLUDED FROM COVERAGE.

Part III – DATA GATHERING & STORAGE

6. Please check which of the following types of third party client/consumer/customer/user data the Company collects, stores, manages, or processes NOT including data provided by employees as part of their employment files?

- Social Security Numbers, Driver's License/Passport Numbers, Credit History/Reports/Ratings, Email Addresses, Date of Birth, Bank Account Numbers, Educational Records, Intellectual Property, Financial Reports/Records, Mother's Maiden Name, Protected Health Information, Government/Tax ID Numbers, UserID & Passwords, Payment Card Numbers, Background Check Information

7. How many unique individuals' records does the Company store, hold or process in a year containing the above-selected information?

8. Is the Company a covered entity or business associate as defined in HIPAA?

If Yes, please provide answers to the following questions:

- a) Is the Company in compliance with the HIPAA Privacy Rule?
b) Is the Company in compliance with the HIPAA Security Rule?
c) e-PHI is encrypted:
d) How frequently does the Company evaluate & document its business associates' HIPAA compliance?

9. Is the Company covered under the Graham-Leach-Bliley Act (GLBA)? Yes No
If Yes, please answer to the following questions:
- a) Is the Company GLBA compliant?
 Yes No
- b) How frequently does the Company evaluate & document the control environment of its 3rd party vendors?
 more frequently than annually annually less frequently than annually
10. Does the Company accept payment cards or any form of electronic payment? Yes No
If Yes, please provide the following information:
- a) How many debit, credit, or payment card transactions does the Company process annually? _____
- b) PCI DSS merchant level
 1 2 3 4
- c) What % of the Company's revenues are from online sales? _____ %
- d) Does the Company retain payment card data for recurring customer charges?
 Yes No
- e) Does the Company make its customers aware that their payment data is being retained when they provide the information?
 Yes No N/A
- f) Are all of the Company's payment card terminals chip-and-pin?
 Yes No
- g) Is the Company presently PCI DSS Compliant?
 Yes No
If Yes, please provide the most recent evaluation date: __/__/____
If No, please detail the Company's noncompliance on a separate attachment, including any steps taken to rectify such situation.
11. Does the Company publish, sell, or share individual subscriber or user identifiable information with other internal or external entities? Yes No
If Yes, detail the Company's activities in this regard on a separate attachment including the data gathered, records involved, revenues derived from such activities and regulatory oversight/limitations of such activities.
12. Indicate in the boxes below if the sensitive data the Company protects is stored and/or accessed via any of the following:
- Employee Owned Devices
Does the Company require and enforce password security measures for these devices? Yes No
Does the Company require encryption of sensitive data accessed on these devices? Yes No
- Paper Files at the Company's Locations
Is physical access to sensitive data restricted? Yes No
Does the Company train employees with respect to handling sensitive physical documents? Yes No
- Paper Files and/or Unencrypted Storage Mediums (tapes, flash drives, CD Roms, etc.) at Vendor Locations
Is the location physically secure? Yes No
Is the location actively monitored? Yes No
- Unencrypted Storage Mediums (tapes, flash drives, CD Roms, etc.) at the Company's Locations
Are these devices allowed to leave the Company's premises? Yes No
- Company Owned Mobile Devices (including, but not limited to laptops, tablets, smartphones, etc.)
Does the Company require and enforce password security measures for these devices? Yes No
Can these devices be remotely wiped in the event they are lost or stolen? Yes No
- Cloud-Based Products/Services
Please complete questions 32 – 36 on page 6. of this application.

Part IV –CONTROLS & PROCEDURES

Network Security

13. Has a network security assessment or audit been conducted within the past 12 months? Yes No
If Yes, please provide the following:
a) Date the last audit was completed? __/__/____
b) Please attach a copy of the assessment or audit.
c) Has the Company since complied with all recommendations from the audit?
 Yes No
d) Please detail the audit recommendations that remain unaddressed: _____

14. Does the Company conduct periodic intrusion detection, penetration or vulnerability testing? Yes No
If Yes, please provide the following details:
a) How frequently is the vulnerability testing performed?
 more frequently than annually annually less frequently than annually
b) The testing is performed by:
 Vendors Internal IT Both
c) Does the Company utilize a 24/7 managed intrusion detection?
 Yes No
d) Intrusion detection is performed by:
 Vendors Internal IT Both
15. Is network firewall technology used to prevent unauthorized access to internal networks at:
a) Public internet access points? Yes No
b) Internal network routers/switches? Yes No
c) Company computers? Yes No
16. Are patches and updates routinely implemented on the Company network devices and applications (including, but not limited to routers, bridges, firewalls, etc.) to mitigate current vulnerabilities? Yes No
If Yes, please provide the following details:
a) How frequently does this take place?
 monthly quarterly semi-annually annually less frequently than annually
b) The implementation is performed by:
 Vendors Internal IT Both
17. Are patches and updates routinely implemented on the Company devices (including, but not limited to servers, desktop PCs, laptops, and mobile devices, etc.) to mitigate current vulnerabilities? Yes No
If Yes, please provide the following details:
a) How frequently does this take place?
 monthly quarterly semi-annually annually less frequently than annually
b) The implementation is performed by:
 Vendors Internal IT Both
18. Does the Company utilize a wireless network at any Company locations? Yes No
If Yes, please provide the type of wireless network authentication utilized:
 None Password Device Certificate
19. The Company's passwords policy requires:
a) User passwords be changed:
 monthly quarterly semi-annually annually less frequently than annually
b) Some form of password complexity (length, numbers, special characters, etc.)?
 Yes No
20. Is an anti-virus solution currently implemented on the Company's devices (including, but not limited to the Company's servers, desktop PCs, laptops, etc.)? Yes No
If Yes, how frequently is the solution updated?
 daily weekly less frequently than weekly

21. Does the Company's network administrator enforce restrictions regarding installing applications to the Company's computers and mobile devices? Yes No

22. Does the Company utilize Sender Policy Framework (SPF) to validate emails? Yes No

Business Continuity

23. Are the Company's primary mission critical systems fault tolerant? Yes No

24. How frequently are the Company's mission critical systems backed up?
 hourly daily weekly monthly less frequently than monthly

25. Does the Company maintain a formal:
- a) Disaster recovery plan that it tests annually?
 Yes No
 - b) Incident Response Plan?
 Yes No
 - c) Does either plan include procedures to be followed in the event of a Security Disruption?
 Yes No
 - d) Does either plan include procedures to be followed in the event of a Data Compromise?
 Yes No

Data Governance

26. Does the Company maintain a Company-wide policy covering records and information management compliance? Yes No

If Yes, please provide the following details:

- a) Does it include enforceable provisions for non-compliance by employees, contractors, and third-party providers/partners?
 Yes No
- b) Has the policy been approved by the Company's Board of Directors?
 Yes No
- c) Does it consolidate Company-wide responsibility for those functions with a dedicated individual?
 Yes No
- d) If Yes to c) above, to whom does that individual report?
 CIO CEO CFO Board of Directors CTO Other: _____

27. Does the Company's human resource department require a full background check (Criminal, Educational, Drug, and Work History) for all:

- a) Prospective employees? Yes No
- b) Temporary employees? Yes No
- c) Independent contractors? Yes No

28. Does the Company's security awareness program include:

- a) Mandatory classes with measured testing for all employees that may be expected to access, handle or process sensitive customer data as part of their assigned job responsibilities? Yes No
- b) Routine network security awareness training for all employees? Yes No

29. Does the Company follow established procedures for both "friendly" and "adverse" employee departures that include an inventoried recovery of all information, assets, user accounts, and systems previously assigned to each individual during their full period of employment? Yes No

30. Are formal processes in place to ensure that network privileges are revoked in a timely manner following an employee's termination or resignation? Yes No

31. Does the Company post a privacy policy on its Internet website? Yes No

If Yes, please provide the following details:

- a) Has the policy been reviewed by a qualified attorney?
 Yes No
- b) When was this policy last updated? ___/___/___

42. Does the Company publish any books, journals, movies, or music as part of its business? Yes No
43. Please select all that apply for the Company's online presence:
 Website Bulletin Board(s) or chat room(s) on the Company website Social Media (facebook, Twitter, etc.)
 Company Blog User Supplied Content (forums, reviews, etc.)
44. Does the Company use third party content such as graphics, images, music, or video on its website? Yes No
If Yes, does the Company always obtain written licenses and consent agreements for the use of these materials?
 Yes No
45. Does the Company have an established procedure for editing or removing content from its website that might be construed as libelous, slanderous, or infringing on the intellectual property rights of others (including, but not limited to copyrights, trademarks, trade names, etc.)? Yes No
46. How often does the Company use an agency for its online content creation?
 Always Sometimes Never

Part VII – MATERIAL CHANGE AND FRAUD WARNINGS

A. MATERIAL CHANGE

If there is any material change in the answers to the questions in this Application prior to the Inception Date of any policy that may be issued, the Company must notify us in writing and any outstanding quotation or binder may be modified or withdrawn. The undersigned Officer of the Company declares that to the best of his or her knowledge the statements set forth herein are true and correct and that reasonable efforts have been made to obtain sufficient information from each and every Insured proposed for this insurance to facilitate the proper and accurate completion of this Application. The signing of this Application does not bind the undersigned to purchase the insurance. The **Insured** represents that the particulars and statements contained within the **Application** are true, complete, accurate, and agrees that this Policy is issued in reliance on the truth of that representation, and that such particulars and statements, which are deemed to be incorporated into and to constitute part of this Policy, are the basis of this Policy. In the event of any material misrepresentations, untruth, or other omission in connection with any of the statements or facts in the **Application**, the knowledge of one **Insured** will not be imputed to another **Insured**; provided, however, this Policy will be void with respect to:

- (1) any **Employee** who knew of such misrepresentation, untruth, or omission; and
- (2) the **Company**, but only if an officer, director, managing member, partner or similar executive of the **Company** knew of such misrepresentation, untruth or omission.

B. FRAUD WARNINGS

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.

ALABAMA, ARKANSAS, LOUISIANA, RHODE ISLAND AND WEST VIRGINIA FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

COLORADO FRAUD WARNING: 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.

D.C. FRAUD WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

FLORIDA FRAUD WARNING: 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.

KENTUCKY FRAUD WARNING: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

MAINE FRAUD WARNING: 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 or denial of insurance benefits.

MARYLAND FRAUD WARNING: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who 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.

NEW JERSEY FRAUD WARNING: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NEW MEXICO FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to civil fines and criminal penalties.

OHIO FRAUD WARNING: Any person who, with the intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

OKLAHOMA APPLICANTS: Warning: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

OREGON FRAUD WARNING: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto may be guilty of a fraudulent insurance act, which may subject such person to prosecution for insurance fraud.

PENNSYLVANIA 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.

TENNESSEE FRAUD WARNING: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

VIRGINIA AND WASHINGTON FRAUD WARNING: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

NEW YORK 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 shall also be subject to a civil penalty not to exceed five thousand dollars (\$5,000.00) and the stated value of the claim for each such violation.

This Application must be signed by the Chairman of the Board, President, Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Information Officer or functional equivalent of the Company.

Signature _____

Title _____ **Date** _____