Cyber & Data Breach Insurance Application

Business Information

Company: ____

Address: ____

Contact: ____

Phone: ______________________ Email: ______________________________

Year Established: ____________ Website: ______________________________

Business Description: ______________________________________

NAICS Code: ______________________________ (see www.naics.com/search.htm)

Gross Revenue: ______________________ Cost of Goods Sold (if applicable): ______________________

Number of Employees: ______________ Number of Independent Contractors (if any): ______________

Risk Assessment

1.) Do you have anti-virus software installed and enabled on all desktops, laptops and servers (excluding database servers) and it is updated on a regular basis? ○ Yes ○ No

2.) Do you implement encryption on laptop computers, desktop computers and other portable media devices? ○ Yes ○ No

3.) Do you have firewalls installed on all external gateways? ○ Yes ○ No

4.) Do you, or your outsourced service, make regular back-ups, at least weekly, of all critical data and store the backups offsite or in a fire-proof safe? ○ Yes ○ No

   a. If yes, are data backups disconnected from and inaccessible through the organization's network? ○ Yes ○ No

   b. If yes, are all data backups secured with different access credentials from other administrator credentials? ○ Yes ○ No

   c. If yes, are backups regularly tested to confirm restoration/recovery of key server configurations and data? ○ Yes ○ No

5.) Do you store medical records or Protected Health Information (PHI)? ○ Yes ○ No

   a. If yes, do you conduct reviews to ensure compliance with all relevant Health Insurance Portability & Accountability Act (HIPPA) legislation? ○ Yes ○ No

   b. If yes, is all PHI transmitted over open networks and / or stored on portable devices encrypted? ○ Yes ○ No

6.) Do you collect, process, store, transmit or have access to any Payment Card Information (PCI), Personally Identifiable Information (PII), or Protected Health Information (PHI), other than your employees? ○ Yes ○ No

   a.) If, yes what is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)? ______________________________

   b.) If yes, how many PII or PHI records do you collect, process, store, transmit or have access to? ______________

7.) Do you require a secondary means of communication to validate the authenticity of funds transfers (ACH, wire, etc.) requests before processing a request in excess of $25,000? ○ Yes ○ No

8.) Does your business have a cyber security awareness program? ○Yes ○No

a.) If yes, does it include training to make employees aware of phishing? ○Yes ○No

b.) If yes, do you complete regular phishing simulation testing exercises? ○Yes ○No

c.) If yes, how often do you complete these tests?
○Annually
○Quarterly
○Monthly
○Not Applicable

9.) Does your business have a written breach incident response plan? ○Yes ○No

a.) If yes, does the plan include specifications for a ransomware event? ○Yes ○No

10.) Does your email system:

a.) Alert users that the email originated from outside the organization? ○Yes ○No

b.) Utilize a tool to filter or scan incoming emails for malicious attachments or links? ○Yes ○No

If yes, please identify the product used to filter or scan____

11.) Is a protective Domain Name Service (DNS) utilized that prevents access to domains known to be malicious? ○Yes ○No

12.) Has Remote Desktop Protocol (RDP) been disabled? ○Yes ○No

a.) If no, is the RDP server located within the Demilitarized Zone (DMZ?) ○Yes ○No

b.) If no, is the RDP only accessible via a VPN? ○Yes ○No

c.) If no, is multi-factor authentication (MFA) used for all RDP connections? ○Yes ○No

13.) Is multi-factor authentication (MFA) required for:

a.) All privileged user accounts? ○Yes ○No

b.) All remote network connections? ○Yes ○No

14.) Is a process in place to identify and install critical software security patches within 30 days? ○Yes ○No

15.) Are the following in place:

a.) Next-Generation Anti-Virus (NGAV)? ○Yes ○No

b.) Endpoint Detection and Response (EDR) Tools? ○Yes ○No

If yes, to a or b above, please describe: ____

16.) Do you enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right? ○Yes ○No

17.) Within the last three years, have you suffered a cyber incident? ○Yes ○No

18.) Within the last three years, have you been the subject of any complaints concerning the content of your website, advertising materials, social media or other publications? ○Yes ○No

19.)After full inquiry, are you aware of any breach, hacking, release of data, violation of any breach regulation or law, or any circumstance, which may give rise to a claim under the insurance sought here? ○Yes ○No

20.) Has any claim, compliant, demand or regulatory proceeding been made or initiated against you? ○Yes ○No

Current Cyber Insurer: ____________________________________ Effective Date: ________________________________

Limits: ________________________ Deductible: ________________________ Premium: __________________

Applicant hereby warrants and represents that the statements and answers made above are true, and applicant has not omitted or misrepresented any information.

Signed: ________________________________ Title: _________________________ Date: __________________________

Please submit your completed form to hello@coverlink.com and we will get to work on your policy right away.

coverlink
INSURANCE