CRC Group
Wholesale & Specialty

Cyber Liability Insurance Application

GENERAL INFORMATION

1. Full Name of Applicant: _____
2. Principal Address: _____
3. Nature of Business (Industry): _____
4. Primary Corporate Website Address: _____
5. Total Employee Count: _____
6. Annual Gross Revenues – Most recent 12 months: _____ Projected Next 12 Months: _____
7. Please attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant Please describe (1) the nature of operations of each such subsidiary, affiliated company or entity, (2) its relationship to the Applicant and (3) the percentage of ownership by the Applicant

   _____

   _____
8. Do you engage in any of the following business activities? (select all that apply)

   ☐ Adult Content ☐ Cannabis ☐ Cryptocurrency or Blockchain
   ☐ Debt collection agency ☐ Gambling ☐ Managed IT service provider (MSP or MSSP)
   ☐ Payment Processing (e.g., as a payment processor, merchant acquirer, or Point of Sale system vendor)
   ☐ None of the above
9. Within the Applicant's organization, who is responsible for network security?
   Name: _____ Title: _____
   Email Address: _____ Phone Number: _____

DATA COLLECTION INFORMATION

1. Estimate number of unique personally identifiable records maintained (including records stored by third-party providers)

   ☐ 0 – 250,000 ☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000
   ☐ 1,000,001 – 2,500,000 ☐ 2,500,001 – 5,000,000 ☐ 5,000,001 – 10,000,000
   ☐ 10,000,001 +

   PII includes any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

2. Do you deal with protected health information as defined by HIPAA? ☐ Yes ☐ No
   a. If "Yes", do you have procedures and audit practices in place to ensure compliance under the rules and regulations of HIPAA, including the encryption of any electronically transmitted record
3. Do you deal with biometric information or data such as fingerprints, voiceprints, facial, hand iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? ☐ Yes ☐ No
   a. If "Yes", have you confirmed compliance with applicable federal, state, local and foreign laws?
4. Do you accept credit or debit card payments ☐ Yes ☐ No
5. If applicable, do you deploy either end-to-end or point-to-point encryption technology on all of you point of sale terminals? ☐ Yes ☐ No

SECURITY CONTROLS

1. Do you require multi-factor authentication for:
   a. All remote access to the network including any remote desktop protocol connections? ☐ Yes ☐ No
   b. All Web based email accounts? ☐ Yes ☐ No
   c. Local and remote access to privileged user/network administrator accounts? ☐ Yes ☐ No
   d. Internal and external access to cloud based back-ups? ☐ Yes ☐ No
2. Do you use a commercially available and regularly updated firewall and anti-virus protection system for all your computer systems? ☐ Yes ☐ No
3. Do you use intrusion detection software to detect unauthorized access to your computer systems? ☐ Yes ☐ No
4. Do you filter or scan incoming emails for potentially malicious attachments and links? ☐ Yes ☐ No
   a. If "Yes", do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user?_____
5. Are you compliant with the Payment Card Industry (PCI) Data Security Standards? ☐ Yes ☐ No
6. Do you implement SPF, DKIM and DMRAC to protect against phishing messages? ☐ Yes ☐ No
7. Do you use Office 365? ☐ Yes ☐ No
   a. If "Yes", do you use the Office 365 Advanced Threat Protection add-on? _____
8. Do you regularly monitor security vulnerabilities and appropriately patch and upgrade systems & applications? ☐ Yes ☐ No
   a. Apply security patches within 30 days of release? ☐ Yes ☐ No
9. Is your critical business data backed-up and stored in a secure location? ☐ Yes ☐ No
   a. if yes, how often:
   ☐ Daily ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Every 6 Months
   b. Does the backup solution include all the following characteristics: kept in a cloud service protected by MFA, has been tested in the last 6 months, and can be used to restore essential network functions within 3 days of a widespread malware or ransomware attack? ☐ Yes ☐ No
   c. Do you use 3-2-1 backup procedures? Two different media storage types and one copy off site for disaster recovery? ☐ Yes ☐ No
10. Do you test the successful restoration and recovery of key server configurations and date from backups? ☐ Yes ☐ No
11. Do you use a cloud provider to store data or host applications? ☐ Yes ☐ No
    a. If "Yes", please provide the name of the cloud provider: _____
12. Do you encrypt private or sensitive information stored on the network or cloud? ☐ Yes ☐ No
13. Do you encrypt private or sensitive information stored on mobile devices? ☐ Yes ☐ No
14. Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? ☐ Yes ☐ No
    If "Yes", please provide the name of your EDR provider: _____
15. Are employees required to undergo annual security training? ☐ Yes ☐ No
16. Do you have controls in place which require all fund and wire transfers over $25,000 to be authorized and verified by at least two employees prior to execution? ☐ Yes ☐ No
17. Does the applicant provide data processing, storage, hosting, or Managed Security Services Provider (MSSP) services to third parties? ☐ Yes ☐ No
18. Has there been a vulnerability assessment in the past 18 months? ☐ Yes ☐ No
19. Do you have a tested business continuity/disaster recovery program in place? ☐ Yes ☐ No

LOSS/CLAIMS INFORMATION

1. In the past 3 years, has the Applicant or any other person or organization proposed for this insurance:
   a. Received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the Applicant's network? ☐ Yes ☐ No
   b. Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? ☐ Yes ☐ No
   c. Notified customers, clients or any third party of any security breach or privacy breach? ☐ Yes ☐ No
   d. Received any cyber extortion demand or threat? ☐ Yes ☐ No
   e. Sustained any unscheduled network outage or interruption for any reason? ☐ Yes ☐ No
   f. Sustained any property damage or business interruption losses as a result of a cyber-attack? ☐ Yes ☐ No
   g. Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? ☐ Yes ☐ No
2. Is the Applicant aware of any fact, circumstance, situation, event, or Wrongful Act which reasonably could give rise to a Cyber Event, Loss, or a Claim being made against them that would fall within the scope of the Policy for which the Applicant is applying? ☐ Yes ☐ No
3. In the past 3 years, has any service provider with access to your network or computer system(s) sustained an unscheduled network outage or interruption lasting longer than 4 hours? ☐ Yes ☐ No

   If "Yes", did you experience an interruption in business as a result of such outage of interruption?

If answered yes to any of the above, please attach full details for each yes answer on a separate attachment.

CERTIFICATION AND SIGNATURE

The Applicant has read the foregoing and understands that completion of this application does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this application is complete and correct to the best of the Applicant's knowledge and belief, and that all particulars which may have a bearing upon acceptability as an insurance risk have been revealed.

It is understood that this application shall form the basis of the contract should the Underwriter approve coverage, and should the Applicant be satisfied with the Underwriter's quotation. It is further agreed that, if in the time between submission of this application and the requested date for coverage to be effective, the Applicant becomes aware of any information which would change the answers furnished in response to any question of this application, such information shall be revealed immediately in writing to the Underwriter.

This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

Print or Type Applicant's Name:_____ Title of Applicant: _____

Signature of Applicant: _____ Date Signed by Applicant: _____