CID Insurance Programs Inc. DBA CID Insurance Services

Cyber Insurance Questionnaire

Section I: General Information

1. Name of Applicant: _____
2. Address: _____

   City: _____ State: _____ Zip: _____

   Phone: _____ Website Address: _____ Email Address: _____
3. Date established: _____
4. Is the Applicant controlled, owned, affiliated or associated with any other firm, corporation or company? ❑Yes ❑No

   If Yes, please provide names(s) and relationship(s): _____
5. Does the Applicant have any subsidiaries? ❑Yes ❑No

   If Yes, please list on a separate sheet and advise if coverage is to apply to them.
6. Applicant is: ❑Individual ❑Corporation ❑LLC ❑Non-Profit ❑Partnership
7. Please provide a full description of your business operations:

   _____

   _____

   _____
8. List total gross revenues derived from activities in Question #7 (start-ups please provide best estimates): Gross Revenues

   Last Year: $_____

   Current Year (based on 12 months): $_____

   Forecast for Next Year: $_____
9. Do you collect, store, host, process, use or share any private or sensitive information in either paper or electronic form? Yes ☐ No ☐ N/A ☐

   a. If yes, please provide the approximate number of unique records:
   Paper records: _____ Electronic records: _____
10. Does your business or any of your clients' business activities involve any of the following:

    a. Cannabis Yes ☐ No ☐
    b. Gambling Activities Yes ☐ No ☐
    c. Adult Content Yes ☐ No ☐
    d. Cryptocurrency Yes ☐ No ☐
    e. Public Entities (Towns, Municipalities, Public Schools, etc.) Yes ☐ No ☐
    f. Hospitals (Doctors Offices/Clinics are acceptable) Yes ☐ No ☐
11. Is similar Cyber Liability Insurance currently in force? Yes ☐ No ☐

Name of Carrier	Limit	Retroactive Date (if any)	Deductible	Premium	Policy Term

Section II: Claims Details

1. Has your business suffered a cyber-related loss or experienced compromise of your data or systems in the past 12 months? Yes ☐ No ☐
2. In the past five years, have any claims or legal actions been brought against you related to data breach extortion threat, or any other incident, loss of money, securities, or property involving any alleged social engineering, fraud, or other criminal acts? Yes ☐ No ☐

   a. Have you had less than 3 incidents and $0 in total overall losses? Yes ☐ No ☐
   b. Have you had less than 3 incidents and $25,000 or less in total overall losses? Yes ☐ No ☐
   c. Have you had greater than or equal to 3 incidents and more than $25,000 in total overall losses? Yes ☐ No ☐

3. Do you (including your affiliates, executives, employees, or contractors) currently have knowledge or information of any act, error, omission, or breach of duty related to any: (1) known network intrusion; (2) denial of service attack; or (3) unauthorized loss, release, or disclosure of personally identifiable information in your care, custody, or control? Yes ☐ No ☐

4. Have you ever been the subject of a regulatory action, investigation, or inquiry as a result of the handling sensitive data, including but not limited to a civil investigative demand, consent order, or investigation by an Attorney General (or equivalent) or other industry body? Yes ☐ No ☐

a. Is the matter still open? Yes ☐ No ☐

b. If the matter is closed, were there any findings or fines? Yes ☐ No ☐

Section III: Compliance & Security Details

1. Do you store, transmit, collect, or process any healthcare records? Yes ☐ No ☐ N/A ☐

a. If yes, are you in compliance with HIPAA (Health Insurance Portability and Accountability Act of 1996) Yes ☐ No ☐

2. Do you process, store, or handle credit card transactions? Yes ☐ No ☐ N/A ☐

a. If yes, are you in compliance with PCI DSS (Payment Card Industry Data Security Standard)? Yes ☐ No ☐

b. Is your payment processing fully outsourced? Yes ☐ No ☐

c. How many transactions do you store? _____

3. Do you collect, store, host, process, use or share any 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 reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? Yes ☐ No ☐

4. Do you encrypt information that is stored on mobile computing devices, including but not limited to laptops and smart phones? Yes ☐ No ☐

5. Do employees use Multi-Factor Authentication (MFA) when accessing your network? [Examples of MFA, Google Authenticator, RSA SecureID, Office 365 MFA, Duo, etc.] Yes ☐ No ☐

6. Do you have rules or policies that limit data retention, or processes by which data is routinely disposed of or destroyed? Yes ☐ No ☐

7. Is data encrypted in transit and/or at rest? Yes ☐ No ☐

8. Do you utilize endpoint security software to protect network-connected devices (such as laptops or PCs)? Yes ☐ No ☐

9. Do you utilize intrusion detection and prevention systems for network monitoring and remediation purposes? Yes ☐ No ☐

10. Do you have a process for classifying applications that are critical or important to keep your business running (?business-critical applications?), and plans in place to limit disruption in the event of a cyber incident impacting such applications? Yes ☐ No ☐

Section IV: Agency Information

1. Agency Name: _____
2. Producer: _____
3. Address: _____

City: _____ State: _____ Zip: _____

4. Phone: _____ Email Address: _____