CANNASURE A SUBSIDIARY OF ONE80	**Cannasure Insurance Services, LLC** a subsidiary of One80 Intermediaries 1468 W. 9th St. STE 805 Cleveland, OH 44113 P: 800-420-5757	**Cyber Application NB** Email Applications to: submission@cannasure.com

APPLICANTS INSTRUCTIONS:

All Applicants must complete the relevant sections of this Application in accordance with the specific coverages being requested.
Answer all questions completely. Please attach extra sheets as required. Incomplete or illegible applications may be rejected.
Application must be signed and dated by the owner, partner, or officer no earlier than 90 days before the proposed effective date of coverage.
Please read the statements at the end of this application carefully.

**If there are multiple Business Names, please provide detailed list or organizational chart showing relationship.*

THIS IS AN APPLICATION FOR CLAIMS MADE AND REPORTED INSURANCE. THIS APPLICATION IS NOT A BINDER.

This application for Cyber Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Company to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. Complete all required supplemental forms/applications. "You" and "Your", as used in this application, means the Applicant.

Please refer to the attached Cyber Glossary for an explanation of the cyber security terms that appear in bold face type.

1. GENERAL INFORMATION

Name of Applicant:	
Street Address:	
City, State, Zip:	Phone:
Website:	Fax:
Description of operations:	
Attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant and include a description of (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.	

2. REVENUES

Total gross revenues for the current fiscal year ending / (current projected): **$**

3. RECORDS

a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? ☐ Yes ☐ No

If "Yes", provide the approximate number of unique records (paper and electronic): _____

* Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.

b. Do you collect, store, host, process, control, 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

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. IT DEPARTMENT

This section must be completed by the individual within the Applicant's organization who is responsible for network security. As used in this section only, "you" refers only to such individual.

a. Within the Applicant's organization, who is responsible for network security?

Name:	Title
IT Security Designation(s):	
Email address:	Phone:

b. The Applicant's network security is:
☐ Outsourced; provide the name of your network security provider: _____
☐ Managed internally/in-house

c. If the Applicant's network security is outsourced, are you the main contact for the network security provider named in question **4.b.** above? ☐ Yes ☐ No

If "No", provide the name and email address for the main contact: _____

By signing below, you confirm that you have reviewed all questions in Section 5 of this application regarding the Applicant's ransomware controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to 1) the Company conducting non-intrusive scans of your internet-facing systems / applications for common vulnerabilities, and 2) receiving direct communications from the Company and/or its representatives regarding the results of such scans and any potentially urgent security issues identified in relation to the Applicant's organization.

Signature: _____

Print/Type Name: _____

5. RANSOMWARE CONTROLS

a. Do you pre-screen emails for potentially malicious attachments and links? ☐ Yes ☐ No

If "Yes", select your email pre-screen provider: Choose an item

If "Other", provide the name of your email pre-screen provider: _____

b. Can your users access email through a web application or a non-corporate device? ☐ Yes ☐ No

If "Yes", do you enforce **Multi-Factor Authentication (MFA)**? ☐ Yes ☐ No

c. Do you allow remote access to your network? ☐ Yes ☐ No

If "Yes", do you use **MFA** to secure all remote access to your network, including any **remote desktop protocol (RDP)** connections? ☐ Yes ☐ No

If **MFA** is used, select your **MFA** provider: Choose an item

If "Other", provide the name of your **MFA** provider: _____

d. Do you use a **next-generation antivirus (NGAV)** product to protect all endpoints across your enterprise? ☐ Yes ☐ No

If "Yes", select your **NGAV** provider: Choose an item

If "Other", provide the name of your **NGAV** provider: _____

e. 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", select your **EDR** provider: Choose an item

If "Other", provide the name of your **EDR** provider: _____

f. Do you use **MF**A to protect all local and remote access to privileged user accounts? ☐ Yes ☐ No

g. Do you use a data backup solution that has **all** of the following characteristics: ☐ Yes ☐ No

(1) kept in a cloud service protected by **MFA**;

(2) runs daily; and

(3) can be used to restore essential network functions within 3 days after a widespread malware or ransomware attack?

ADDITIONAL COMMENTS (*Use this space, or attach a separate page, if space is insufficient, to explain any answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.*)

6. PHISHING CONTROLS

Do any of your employees complete social engineering training? ☐ Yes ☐ No

If "Yes":

a. does your social engineering training include phishing simulation? ☐ Yes ☐ No

b. do employees with financial or accounting responsibilities complete training? ☐ Yes ☐ No

c. do employees without financial or accounting responsibilities complete training? ☐ Yes ☐ No

7. LOSS HISTORY

In the past 3 years, has the Applicant or any other person or organization proposed for this insurance experienced one or more of the following: ☐ Yes ☐ No

- Been served with a lawsuit or received a demand, complaint or charge alleging liability for a privacy breach, privacy injury, security breach, intellectual property infringement or reputational harm;
- Been the subject of any government action, investigation or proceedings regarding any alleged violation of privacy law;
- Notified customers, clients or any third party of any security breach or privacy breach;
- Received any cyber extortion demand or threat;
- Sustained any unscheduled network outage or interruption for any reason;
- Sustained any property damage or business interruption losses as a result of a cyber-attack;
- Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud;
- A business interruption as a direct result of an unscheduled network outage or interruption of a service provider computer system; or
- Became aware of any other cyber security or data privacy event, incident or allegation involving or impacting your organization?

If "Yes", please use the Additional Comments section below to describe each claim, allegation or incident you have experienced (or attach a separate page, if space is insufficient). Please also complete a Claim Supplemental Form for each claim, allegation or incident.

ADDITIONAL COMMENTS:

NOTICE TO APPLICANT

The insurance for which you are applying will not respond to incidents about which any person proposed for coverage had knowledge prior to the effective date of the policy nor will coverage apply to any claim or circumstance identified or that should have been identified in question 7 of this application.

The Applicant hereby acknowledges that he/she/it is aware that the limit of liability shall be reduced, and may be completely exhausted, by claim expenses and, in such event, the Company shall not be liable for claim expenses or any judgment or settlement that exceed the limit of liability.

I HEREBY DECLARE that, after inquiry, the above statements and particulars are true and I have not suppressed or misstated any material fact, and that I agree that this application shall be the basis of the contract with the Company.

CERTIFICATION, CONSENT AND SIGNATURE

The Applicant has read the foregoing and understands that completion of this application does not bind the Company 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 a Cyber Insurance risk have been revealed.

By signing below, the Applicant consents to the Company conducting non-intrusive scans of the Applicant's internet-facing systems / applications for vulnerabilities.

It is understood that this application shall form the basis of the contract should the Company approve coverage, and should the Applicant be satisfied with the Company'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 Company.

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 Applicant.

Print or Type Applicant's Name	Title of Applicant
Signature of Applicant	Date Signed by Applicant