

## Basic information

Company name: \_\_\_\_\_

Address: \_\_\_\_\_

*Including Floor, Suite or Unit number*

Website: \_\_\_\_\_ Applicant's email address: \_\_\_\_\_

*Optional*

Annual revenue of last fiscal year: \_\_\_\_\_ Number of company employees: \_\_\_\_\_

Security contact information:

Name: \_\_\_\_\_

Email: \_\_\_\_\_ Phone: \_\_\_\_\_

Industry: \_\_\_\_\_

I confirm that the applicant does NOT operate in any of the following: Cannabis, Online Gambling, Adult Content

## Insurance and claims

Does the applicant currently carry a standalone cyber policy?

Yes  No

- If yes, indicate expiration date: \_\_\_\_\_

**Claim activity** - In the last 5 years, has the company suffered any cyber event, unscheduled network outage over 4 hours, loss or claim that would fall within the scope of the policy for which the applicant is applying?

Yes  No

- If yes, please complete the following details:

Loss amount: \_\_\_\_\_ Date of notice: \_\_\_\_\_

Event description: \_\_\_\_\_

What has the applicant done since the event to prevent future claims? \_\_\_\_\_

The applicant has not had any legal action and/or regulatory action brought or threatened against them in the last five years as a direct result of a cyber event.

The applicant or any other person or organization proposed for this insurance is not 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?

Within the last 3 years, the applicant has not been subject to any complaints concerning the content of its website, advertising materials, social media, or other publications.

## Security Controls

---

1. Multi-factor authentication (MFA) - Does the applicant have multi-factor authentication enabled on email access, remote access & network administration?

Yes  No  I don't know

2. How many PII, PHI or PCI records does the applicant collect, process, store, transmit, or have access to?

No records  <100K  100K-250K  250K-500K  500K-1M  >1M  I don't know

3. How many biometric information records or data (i.e fingerprints, retinal scans, etc.) does the applicant collect, process, store, transmit, or have access to that can be used to uniquely identify a person?

No records  <100K  100K-250K  250K-500K  500K-1M  >1M  I don't know

4. Does the applicant keep offline backups for all critical data that are disconnected from its network or store backups with a cloud service provider?

Yes  No  I don't know

- If yes, how frequently does it run?

Continuously  Daily  Weekly  Monthly  More than monthly  I don't know

5. Does the applicant implement encryption on laptop computers, desktop computers, and other portable media devices for all sensitive information?

Yes  No  I don't know

6. What is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)?

No payment card transactions  <100K  100K-500K  500K-1M  >1M  I don't know

- If relevant, is the applicant or their outsourced payment processor PCI-DSS compliant?

Yes, applicant does not use outsourced payment processor  Yes  No  I don't know

7. Does the applicant require a secondary means of communication to validate the authenticity of funds transfers (ACH, wire, etc.) requests by at least 2 employees before processing a request in excess of \$25,000?

Yes  No  I don't know

8. Does the applicant enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right?

Yes  No  I don't know