

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

This application for TechGuard® Cyber Liability Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Underwriter 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 Primary Applicant: _____

Business Address: _____

Phone: _____

Website (**List all websites/ domains owned/operated by all entities seeking coverage**): _____

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.

Does the Applicant engage in any of the following industries or offer these services to others for a fee? Yes No

Adult content, autonomous driving software or devices, background screening, credit reporting, consumer generated content platforms, credit card administration, crowdfunding platforms, cryptocurrency, tokens, NFTs, wallets or exchanges, dating platforms, debt collection software, digital distribution of music/video, e-tobacco devices, hardware components and embedded hardware, loan origination software, payday loan platforms, revenue cycle management, semiconductors, smartphones, tax software, user authentication / verification / single-sign-on software, utility billing software and devices, voting software and hardware, pay-per-click services, unmanned aerial vehicle units or services.

Does the Applicant engage in any of the following industries or offer these services to others for a fee? Yes No

Artificial intelligence / machine learning, call center/telemarketing, cannabis software, cloud service provider, computer recycling / refurbish / resale, data analysis – healthcare and financial, data destruction, data management - PII exposure, e-commerce software, e-discovery software, electronic health records (EHR), electronic medical records hosts, emergency communications, financial software (non-trading), financial trading software, gaming/gambling software, IOT (internet of things) devices, lead generation, mass communication software (SMS texting, masked phone number services), medical/health related software, mobile banking software, outsourced administration (benefits administration, billing, TPA, verification), payment solutions / payment processing software, POS hardware development, robotics design and automation software, security software, social media, video game software.

2. TOTAL GROSS REVENUES

Current Full Fiscal Year: _____

\$ _____

3. RECORDS

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):

0-499k 500k-999k 1M+

4. RANSOMWARE CONTROLS

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

If "Yes", do you require **Multi-Factor Authentication (MFA)** to secure all remote access to your network, by employees and third parties, including **VPNs (Virtual Private Network)**, **RDP (Remote Desktop Protocol)**, **RDWeb** or any **RMM (Remote Management and Monitoring)** applications? Yes No

b. Do you use **MFA** to protect all local and remote access to privileged user accounts? Yes No

5. 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:

- 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;

- Received any complaints or written demands, or been a subject of litigation or any governmental investigation, inquiry or other proceedings involving allegations of professional errors or omissions;
- Received knowledge of any wrongful act, error, omission, security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim;
- 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, lasting longer than 4 hours;
- 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?

Yes No

6. 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.

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

Name:

Phone:

Title:

Email address:

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 5 of this application.

NOTICE TO NEW YORK APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

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 Insurer 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 Underwriters.

CERTIFICATION, CONSENT 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 a TechGuard® Cyber Liability Insurance risk have been revealed.

By signing below, the Applicant consents to the Insurer 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 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 |

California Fraud Warning

For your protection, California law requires the following to appear on this form: Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

The following glossary is provided to assist you in completing your cyber application correctly and completely.

Multi-Factor Authentication (MFA) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print). MFA for remote email access can be enabled through most email providers.

Common MFA providers for remote network access:

Okta; Duo; LastPass; OneLogin; and Auth0.

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Remote Desktop Web (RDWeb), also known as Microsoft Remote Desktop Web Access, is a service that provides remote access to corporate resources through a web portal. Resources may include remote desktop access and other applications published on the portal.



Remote Monitoring and Management (RMM) tools allow IT providers to remotely manage and monitor network environments. RMM tools may include remote access, patch management, and reporting functionalities.

Common Providers: ConnectWise and ManageEngine

Virtual Private Network (VPN) encrypts connections between a remote device and an internal network. VPNs are utilized to allow systems from outside the network to connect to internal resources.

Common Providers: Fortnet, Cisco, and Palo Alto VPN Appliances

