

Cyber Liability Insurance Application

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 Applicant:			
Street Address:			
City, State, Zip:		Phone:	
Website:		Fax:	
Square footage for all locations owned or leased by the Applicant (If applying for General Liability Insurance):			
2. FORM OF BUSINESS			
a. Applicant is a(an):	<input type="checkbox"/> Individual	<input type="checkbox"/> Corporation	<input type="checkbox"/> Partnership <input type="checkbox"/> Other: _____
b. Date established:			
c. Description of operations:			
d. Total number of employees:			
e. 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.			
3. REVENUES			
	<u>Current Fiscal Year</u> ending / (current projected)	<u>Last Fiscal Year</u> ending /	<u>Two Fiscal Years ago</u> ending /
Total gross revenues:	\$	\$	\$
4. RECORDS			
<p>a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", provide the approximate number of unique records:</p> <p>Paper records: _____ Electronic records: _____</p> <p>*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.</p>			
<p>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? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>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? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
<p>c. Do you process, store, or handle credit card transactions? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", are you PCI-DSS Compliant? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
5. IT DEPARTMENT			
<i>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.</i>			
a. Within the Applicant's organization, who is responsible for network security?			
Name:			

Title:			
Phone:		Email address:	
IT Security Designation(s):			
<p>b. The Applicant's network security is: <input type="checkbox"/> Outsourced; provide the name of your network security provider: _____</p> <p style="text-align: center;"><input type="checkbox"/> Managed internally/in-house</p>			
<p>c. If the Applicant's network security is outsourced, are you the main contact for the network security provider named in question b. above? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "No", provide the name and email address for the main contact: _____</p>			
d. How many IT personnel are on your team?			
e. How many dedicated IT security personnel are on your team?			
<p>By signing below, you confirm that you have reviewed all questions in Sections 6 through 8 of this application regarding the Applicant's security controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to 1) the Insurer conducting non-intrusive scans of your internet-facing systems / applications, and 2) receiving direct communications from the Insurer and/or its representatives regarding the results of such scans and any potentially urgent security issues identified in relation to the Applicant's organization.</p> <p>Print/Type Name: _____</p> <p>Signature: _____</p>			
6. INFORMATION AND NETWORK SECURITY CONTROLS			
<p>a. Do you use a cloud provider to store data or host applications? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", provide the name of the cloud provider: _____</p> <p>If you use more than one cloud provider to store data, specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.</p>			
<p>b. Do you use Multi-Factor Authentication (MFA) to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
<p>c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "No", are the following compensating controls in place:</p> <p>(1) Segregation of servers that store sensitive and confidential information? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>(2) Access control with role-based assignments? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
7. RANSOMWARE CONTROLS			
<p>a. Do you pre-screen emails for potentially malicious attachments and links? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", complete the following:</p> <p>(1) Select your email security provider: _____</p> <p>If "Other", provide the name of your email security provider: _____</p> <p>(2) 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? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
<p>b. Do you allow remote access to your network? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If MFA is used, complete the following:</p> <p>(1) Select your MFA provider: _____</p> <p>If "Other", provide the name of your MFA provider: _____</p> <p>(2) Select your MFA type: _____</p> <p>If "Other", describe your MFA type: _____</p> <p>(3) Does your MFA configuration ensure that the compromise of a single device will only compromise a single authenticator? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
<p>c. Can your users access email through a web application or a non-corporate device? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", do you enforce MFA? <input type="checkbox"/> Yes <input type="checkbox"/> No</p>			
<p>d. Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If "Yes", select your NGAV provider: _____</p> <p>If "Other", provide the name of your NGAV provider: _____</p>			

<p>e. Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise?</p> <p>If “Yes”, complete the following:</p> <p>(1) Select your EDR provider: If “Other”, provide the name of your EDR provider: _____</p> <p>(2) Do you enforce application whitelisting/blacklisting?</p> <p>(3) Is EDR deployed on 100% of endpoints? If “No”, please use the Additional Comments section to outline which assets do not have EDR, and whether any mitigating safeguards are in place for such assets.</p> <p>(4) Can users access the network with their own device (“Bring Your Own Device”)? If “Yes”, is EDR required to be installed on these devices?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>f. Do you use MFA to protect all local and remote access to privileged user accounts?</p> <p>If “Yes”, select your MFA type: If “Other”, describe your MFA type: _____</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>g. Do you utilize a Security Operations Center (SOC)?</p> <p>If “Yes”, complete the following:</p> <p>(1) Is your SOC monitored 24 hours a day, 7 days a week?</p> <p>(2) Your SOC is: <input type="checkbox"/> Outsourced; provide the name of your provider: _____ <input type="checkbox"/> Managed internally/in-house</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>h. Do you use a vulnerability management tool?</p> <p>If “Yes”, complete the following:</p> <p>(1) Select your provider: If “Other”, provide the name of your provider: _____</p> <p>(2) What is your patching cadence? <input type="checkbox"/> 1-3 days <input type="checkbox"/> 4-7 days <input type="checkbox"/> 8-30 days <input type="checkbox"/> 1 month or longer</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>i. Do you use a data backup solution?</p> <p>If “Yes”:</p> <p>(1) Which best describes your data backup solution? <input type="checkbox"/> Backups are kept locally but separate from your network (offline/air-gapped backup solution). <input type="checkbox"/> Backups are kept in a dedicated cloud backup service. <input type="checkbox"/> You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive). <input type="checkbox"/> Other (<i>describe your data backup solution</i>): _____</p> <p>(2) Check all that apply: <input type="checkbox"/> Your backups are encrypted. <input type="checkbox"/> You have immutable backups. <input type="checkbox"/> Your backups are secured with different access credentials from other administrator credentials. <input type="checkbox"/> You utilize MFA for both internal and external access to your backups. <input type="checkbox"/> You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months. <input type="checkbox"/> You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.</p> <p>(3) How frequently are backups run? <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly</p> <p>(4) Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network? <input type="checkbox"/> 0-24 hours <input type="checkbox"/> 1-3 days <input type="checkbox"/> 4-6 days <input type="checkbox"/> 1 week or longer</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>ADDITIONAL COMMENTS (Use this space to explain any “No” answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)</p>	
<p>8. PHISHING CONTROLS</p>	
<p>a. Do any of the following employees at your company complete social engineering training:</p> <p>(1) Employees <u>with</u> financial or accounting responsibilities?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>

(2) Employees <u>without</u> financial or accounting responsibilities? If "Yes" to question 8.a.(1) or 8.a.(2) above, does your social engineering training include phishing simulation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
b. Does your organization send and/or receive wire transfers? If "Yes", does your wire transfer authorization process include the following:	<input type="checkbox"/> Yes <input type="checkbox"/> No
(1) A wire request documentation form?	<input type="checkbox"/> Yes <input type="checkbox"/> No
(2) A protocol for obtaining proper written authorization for wire transfers?	<input type="checkbox"/> Yes <input type="checkbox"/> No
(3) A separation of authority protocol?	<input type="checkbox"/> Yes <input type="checkbox"/> No
(4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the payment or funds transfer instruction/request was received?	<input type="checkbox"/> Yes <input type="checkbox"/> No
(5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the change request was received?	<input type="checkbox"/> Yes <input type="checkbox"/> No

9. PROFESSIONAL SERVICES

a. Describe in detail the professional services for which coverage is desired.	
b. Are you engaged in any business or profession other than described in Question 9.a? If "Yes", provide an explanation below and an estimate of total revenues derived from such other business or profession:	<input type="checkbox"/> Yes <input type="checkbox"/> No

c. For the revenues listed in Question 3, provide the approximate percentage derived from performing the following services for others:	
<ul style="list-style-type: none"> • Computer/Telecommunications Systems Consulting/Design: _____% • Hardware/Software/System Sales, Installation and/or Training: _____% • Development, Publication or Reproduction of Prepackaged Software: _____% • Custom Software Development, Installation and/or Training: _____% • Hardware/Firmware Development or Assembly (including Robotics): _____% • Personnel Outsourcing/Contract Services: _____% • Facilities Outsourcing, Server Farm, Data Storage: _____% • Data Recovery, Disaster Planning Services: _____% • Website Consulting and/or Development: _____% • Internet Time Leasing, Web Server Farming, Website Hosting: _____% • Internet Access Provider/Service Provider: _____% • Application Service Provider: _____% • Other (please describe): _____% 	TOTAL REVENUE: 100%

d. Indicate by percentage of your overall services the type(s) of businesses to which you provide services:	
<ul style="list-style-type: none"> <li style="width: 50%;">• Aeronautics _____% <li style="width: 50%;">• Manufacturing _____% <li style="width: 50%;">• Communications _____% <li style="width: 50%;">• Government/Military _____% <li style="width: 50%;">• Consumer/Home use _____% <li style="width: 50%;">• Government/Non-Military _____% <li style="width: 50%;">• Engineering _____% <li style="width: 50%;">• Office _____% <li style="width: 50%;">• Healthcare/Medical _____% <li style="width: 50%;">• Retail/Wholesale _____% <li style="width: 50%;">• Internet _____% <li style="width: 50%;">• Other (state): _____% 	TOTAL: 100%

e. List your five (5) largest jobs or projects during the past three (3) years:				
<u>Project/Client Name</u>	<u>Date Services Began</u>	<u>Nature of Services Performed</u>	<u>Revenue</u>	<u>% of Total Gross Revenue</u>

10. CONTRACTUAL INFORMATION

a. Do you use a written contract/agreement with clients describing the services provided?

- Always Most of the time Some of the time Never

Attach a sample copy of your written contract/agreement.

b. Do your contracts contain indemnification or hold harmless clauses inuring to your benefit?

- Always Most of the time Some of the time Never

c. Do your contracts contain limitation of liability clauses or disclaimers inuring to your benefit?

- Always Most of the time Some of the time Never

d. Do your contracts contain an exclusion of consequential damages inuring to your benefit?

- Always Most of the time Some of the time Never

e. Do your contracts contain guarantees or warranties?

- Always Most of the time Some of the time Never

f. Do you assume liability for others under your contracts?

- Always Most of the time Some of the time Never

g. Does the Applicant ever enter into contracts where the fees for services are contingent upon the client achieving cost reductions or improved operating results?

- Yes No

11. MEDIA LIABILITY

a. Do you use, disseminate or display any material or content (e.g., music, graphics or video streams) of others on your website, media material or media platforms?

- Yes No

If "Yes", do you always obtain the necessary rights, licenses, releases & consents for the use of any material/content of others?

- Yes No

Describe below your process for obtaining the necessary rights, licenses, releases & consents for the use of any material/content of others.

b. Describe your policies and procedures for identifying, editing and/or removing defamatory or infringing content from your websites, media material or media platforms.

12. LOSS HISTORY

If the answer to any question in 12.a. through 12.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

a. In the past three (3) years, has the Applicant or any other person or organization proposed for this insurance:

(1) 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?

- Yes No

(2) Received any complaints or written demands or been a subject of 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

(3) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation?

- Yes No

(4) Notified customers, clients or any third party of any security breach or privacy breach?

- Yes No

(5) Received any cyber extortion demand or threat?

- Yes No

(6) Sustained any unscheduled network outage or interruption for any reason?

- Yes No

(7) Sustained any property damage or business interruption losses as a result of a cyber-attack?

- Yes No

(8) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud?	<input type="checkbox"/> Yes <input type="checkbox"/> No
b. Do you or any other person or organization proposed for this insurance have 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
c. In the past three (3) years, has any service provider with access to the Applicant's network or computer system(s) sustained an unscheduled network outage or interruption lasting longer than four (4) hours? If "Yes", did the Applicant experience an interruption in business as a result of such outage or interruption?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No

13. GENERAL LIABILITY LOSS HISTORY

Please answer questions 13.a. & 13.b. below only if General Liability Coverage is desired.

If the answer to question 13.a. or 13.b. is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

a. Does the Applicant or any other person or organization proposed for this insurance have knowledge of any situation(s), circumstance(s) or allegation(s) of bodily injury, property damage or personal and advertising injury that may give rise to a claim?	<input type="checkbox"/> Yes <input type="checkbox"/> No
b. In the past five (5) years, has any claim for bodily injury, property damage or personal and advertising injury ever been made against the Applicant or any other person or organization proposed for this insurance?	<input type="checkbox"/> Yes <input type="checkbox"/> No

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 12. and question 13. 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 common 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.