



## TechGuard® 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.*

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. Please attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant. Please describe (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			
	<b>Current</b> Fiscal Year ending / (current projected)	<b>Last</b> Fiscal Year ending /	<b>Two</b> Fiscal Years ago ending /
Total gross revenues:	\$	\$	\$
4. RECORDS			
a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? If "Yes", please provide the approximate number of unique records: Paper records: _____ Electronic records: _____ <b>*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>			<input type="checkbox"/> Yes <input type="checkbox"/> No
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? 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 <input type="checkbox"/> Yes <input type="checkbox"/> No
c. Do you process, store, or handle credit card transactions? If "Yes", are you PCI-DSS Compliant?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
5. IT DEPARTMENT			
<b><i>This section must be completed by the individual responsible for the Applicant's network security. As used in this section only, "you" refers to the individual responsible for the Applicant's network security.</i></b>			
a. Who is responsible for the Applicant's network security?			
Name:			
Title:			

Phone:		Email address:	
IT Security Designation(s):			
b. The Applicant's network security is: <input type="checkbox"/> Outsourced <input type="checkbox"/> Managed internally/in-house			
c. How many IT personnel are on your team?			
d. How many dedicated IT security personnel are on your team?			
<p><b>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 receiving direct communications from the Insurer and/or its representatives regarding potentially urgent security issues identified in relation to the Applicant's organization.</b></p> <p>Print/Type Name: _____</p> <p>Signature: _____</p>			
<b>6. INFORMATION AND NETWORK SECURITY CONTROLS</b>			
a. Do you use a cloud provider to store data or host applications? If "Yes", please provide the name of the cloud provider: _____ If you use more than one cloud provider to store data, please 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.		<input type="checkbox"/> Yes <input type="checkbox"/> No	
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	
c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? If "No", are the following compensating controls in place: (1) Segregation of servers that store sensitive and confidential information? (2) Access control with role-based assignments?		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No	
<b>7. RANSOMWARE CONTROLS</b>			
a. Do you pre-screen emails for potentially malicious attachments and links? If "Yes", 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 <input type="checkbox"/> Yes <input type="checkbox"/> No	
b. Do you allow remote access to your network? If "Yes": (1) Do you use MFA to secure all remote access to your network, including any remote desktop protocol (RDP) connections? If MFA is used, please select your MFA provider: If "Other", please provide the name of your MFA provider: _____		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No	
c. Can your users access email through a web application or a non-corporate device? If "Yes", do you enforce Multi-Factor Authentication (MFA)?		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No	
d. Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? If "Yes", please select your NGAV provider: If "Other", please provide the name of your NGAV provider: _____		<input type="checkbox"/> Yes <input type="checkbox"/> No	
e. Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? If "Yes", please select your EDR provider: If "Other", please provide the name of your EDR provider: _____		<input type="checkbox"/> Yes <input type="checkbox"/> No	
f. Do you use MFA to protect access to privileged user accounts?		<input type="checkbox"/> Yes <input type="checkbox"/> No	
g. Do you use a data backup solution? If "Yes": a. How frequently does it run? <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly b. Estimated amount of time it will take to restore essential functions 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 c. Please check all that apply: <input type="checkbox"/> Backups are encrypted.		<input type="checkbox"/> Yes <input type="checkbox"/> No	

<input type="checkbox"/> Backups are kept separate from your network (offline/air-gapped), or in a cloud service designed for this purpose. <input type="checkbox"/> Backups are secured with different access credentials from other administrator credentials. <input type="checkbox"/> You utilize MFA to restrict access to your backups. <input type="checkbox"/> You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups. <input type="checkbox"/> Your cloud-syncing service is protected by MFA. <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.	
--	--

**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.)

**8. PHISHING CONTROLS**

<p><b>a.</b> Do any of the following employees at your company complete social engineering training:</p> <p>(1) Employees <b>with</b> financial or accounting responsibilities?</p> <p>(2) Employees <b>without</b> financial or accounting responsibilities?</p> <p><b>If "Yes" to question 8.a.(1) or 8.a.(2) above, does your social engineering training include phishing simulation?</b></p>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
<p><b>b.</b> Does your organization send and/or receive wire transfers?</p> <p><b>If "Yes", does your wire transfer authorization process include the following:</b></p> <p>(1) A wire request documentation form?</p> <p>(2) A protocol for obtaining proper written authorization for wire transfers?</p> <p>(3) A separation of authority protocol?</p> <p>(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 <b>before</b> the payment or funds transfer instruction/request was received?</p> <p>(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 <b>before</b> the change request was received?</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No

**9. PROFESSIONAL SERVICES**

<p><b>a.</b> Please describe in detail the professional services for which coverage is desired.</p>	
<p><b>b.</b> Are you engaged in any business or profession other than described in Question 9.a?</p> <p><b>If "Yes", please provide an explanation below and an estimate of total revenues derived from such other business or profession:</b></p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p><b>c.</b> For the revenues listed in Question 3, please provide the approximate percentage derived from performing the following services for others:</p> <ul style="list-style-type: none"> <li>• Computer/Telecommunications Systems Consulting/Design: _____%</li> <li>• Hardware/Software/System Sales, Installation and/or Training: _____%</li> <li>• Development, Publication or Reproduction of Prepackaged Software: _____%</li> </ul>	

- 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. Please indicate by percentage of your overall services the type(s) of businesses to which you provide services:**

• Aeronautics _____%	• Manufacturing _____%
• Communications _____%	• Government/Military _____%
• Consumer/Home use _____%	• Government/Non-Military _____%
• Engineering _____%	• Office _____%
• Healthcare/Medical _____%	• Retail/Wholesale _____%
• Internet _____%	• Other (state): _____%

**TOTAL 100%**

**e. Please list your five (5) largest jobs or projects during the past three (3) years:**

Project/Client Name	Date Services Began	Nature of Services Performed	Revenue	% of Total Gross Revenue

**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  
**Please 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

<p>If “Yes”, do you always obtain the necessary rights, licenses, releases &amp; consents for the use of any material/content of others? Please describe below your process for obtaining the necessary rights, licenses, releases &amp; consents for the use of any material/content of others.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

b. Please 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.

<p>a. In the past three (3) years, has the Applicant or any other person or organization proposed for this insurance:</p> <p>(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?</p> <p>(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?</p> <p>(3) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation?</p> <p>(4) Notified customers, clients or any third party of any security breach or privacy breach?</p> <p>(5) Received any cyber extortion demand or threat?</p> <p>(6) Sustained any unscheduled network outage or interruption for any reason?</p> <p>(7) Sustained any property damage or business interruption losses as a result of a cyber-attack?</p> <p>(8) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud?</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No                    
<p>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?</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>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?</p>	<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.

<p>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?</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>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?</p>	<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 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.

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

The following Cyber Glossary is provided to assist you in completing your application correctly and completely.

**DomainKeys Identified Mail (DKIM)** is an email authentication method that allows senders to associate a domain name with an email message, thus vouching for its authenticity. A sender creates the DKIM by “signing” the email with a digital signature. This “signature” is located in the message's header.

**Domain-based Message Authentication, Reporting & Conformance (DMARC)** is an email authentication protocol that uses Sender Policy Framework (SPF) and DKIM to determine the authenticity of an email message.

**Endpoint application isolation and containment technology** is a form of zero-trust endpoint security. Instead of detecting or reacting to threats, it enforces controls that block and restrain harmful actions to prevent compromise. Application containment is used to block harmful file and memory actions to other apps and the endpoint. Application isolation is used to prevent other endpoint processes from altering or stealing from an isolated app or resources.

**Common Providers:** Authentic8 Silo; BitDefender™ Browser Isolation; CylancePROTECT; Menlo Security Isolation Platform; Symantec Web Security Service

**Endpoint Detection and Response (EDR)**, also known as endpoint *threat* detection and response, centrally collects and analyzes comprehensive endpoint data across your entire organization to provide a full picture of potential threats.

**Common Providers:** Carbon Black Cloud; CrowdStrike Falcon Insight; SentinelOne; Windows Defender Endpoint

**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.

**Next-Generation Anti-Virus (NGAV)** is software that uses predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to detect and prevent malware and fileless non-malware attacks, identify malicious behavior, and respond to new and emerging threats that previously went undetected. For purposes of completing this application, NGAV refers to anti-virus protection that focuses on detecting and preventing malware on each individual endpoint. If your organization has a NGAV solution **AND** you are centrally monitoring and analyzing all endpoint activity, please indicate that you have NGAV & EDR on the application.

**Common Providers:** BitDefender™; Carbon Black; CrowdStrike Falcon Prevent; SentinelOne; Sophos; Symantec

**Offline/Air-gapped backup solution** refers to a backup and recovery solution in which one copy of your organization's data is offline (i.e., disconnected) and cannot be accessed. If a file or system of files has no connection to the internet or a LAN, it can't be remotely hacked or corrupted.



**Powershell** is a cross-platform task automation and configuration management framework from Microsoft, consisting of a command-line shell and scripting language. It is used by IT departments to run tasks on multiple computers in an efficient manner. For example, Powershell can be used to install a new application across your organization.

**Privileged Account Management Software (PAM)** is software that allows you to secure your privileged credentials in a centralized, secure vault (i.e., a password safe). To qualify as PAM, a product must allow administrators to create privileged access accounts; offer a secure vault to store privileged credentials; and monitor and log user actions while using privileged accounts.

**Common Providers:** CyberArk and BeyondTrust.

**Protective DNS Service (PDNS)** refers to a service that provides Domain Name Service (DNS) protection (also known as DNS filtering) by blacklisting dangerous sites and filtering out unwanted content. It can also help to detect & prevent malware that uses DNS tunneling to communicate with a command and control server.

**Common Providers:** Zscaler; Quad9; OpenDNS; and public sector PDNS.

**Remote Desktop Protocol (RDP) connections** 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.

**Security Information and Event Management system (SIEM)** is a subsection within the field of computer security, wherein software products and services combine security information management and security event management. SIEM provides real-time analysis of security alerts generated by applications and network hardware.



**Security Operations Center (SOC)** is a centralized unit that deals with security issues on an organizational and technical level.

**Sender Policy Framework (SPF)** is an email authentication technique used to prevent spammers from sending messages on behalf of your domain. With SPF, your organization can publish authorized mail servers.

**Vulnerability management tool** is a cloud service that gives you instantaneous, global visibility into where your IT systems might be vulnerable to the latest internet threats and how to protect against them. The tool is an ongoing process that includes proactive asset discovery, continuous monitoring, mitigation, remediation and defense tactics to protect your organization's modern IT attack surface from cyber threats.

**Common Providers:** Qualys; InsightVM by Rapid7; and Nessus® by Tenable™