



NetGuard® Plus Cyber Liability Insurance Short Form Application

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

This application for NetGuard® Plus 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:	
2. FORM OF BUSINESS			
a. Applicant is a(an): ☐ Individual ☐ Corporation ☐ Partnership ☐ 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			
	Current Fiscal Year ending / (current projected)	Last Fiscal Year ending /	Two 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: _____ <small>*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.</small>			☐ Yes ☐ 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?			☐ Yes ☐ No ☐ Yes ☐ No
c. Do you process, store, or handle credit card transactions? If "Yes", are you PCI-DSS Compliant?			☐ Yes ☐ No ☐ Yes ☐ No
5. IT DEPARTMENT			
<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>			
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: ☐ Outsourced ☐ 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>By signing below, you confirm that you have reviewed all questions in Sections 6 through 7 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.</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? 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.</p>	☐ Yes ☐ 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)?	☐ Yes ☐ No
<p>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?</p>	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
7. RANSOMWARE CONTROLS	
<p>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?</p>	☐ Yes ☐ No ☐ Yes ☐ No
<p>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: _____</p>	☐ Yes ☐ No ☐ Yes ☐ No
<p>c. 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: _____</p>	☐ Yes ☐ No
<p>d. 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: _____</p>	☐ Yes ☐ No
e. Do you use MFA to protect access to privileged user accounts?	☐ Yes ☐ No
<p>f. Do you use a data backup solution? If "Yes":</p> <p>a. How frequently does it run? ☐ Daily ☐ Weekly ☐ Monthly</p> <p>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? ☐ 0-24 hours ☐ 1-3 days ☐ 4-6 days ☐ 1 week or longer</p> <p>c. Please check all that apply: ☐ Backups are encrypted. ☐ Backups are kept separate from your network (offline/air-gapped), or in a cloud service designed for this purpose. ☐ Backups are secured with different access credentials from other administrator credentials. ☐ You utilize MFA to restrict access to your backups. ☐ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups. ☐ Your cloud-syncing service is protected by MFA. ☐ You have tested the successful restoration and recovery of key server configurations and data</p>	☐ Yes ☐ No

from backups in the last 6 months. ☐ 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		
a. Do any of the following employees at your company complete social engineering training: (1) Employees <u>with</u> financial or accounting responsibilities? (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?		☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
b. Does your organization send and/or receive wire transfers? If "Yes", does your wire transfer authorization process include the following: (1) A wire request documentation form? (2) A protocol for obtaining proper written authorization for wire transfers? (3) A separation of authority protocol? (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? (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?		☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
9. LOSS HISTORY		
If the answer to any question in 9.a. through 9.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.		
a. In the past 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 in 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? (2) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? (3) Notified customers, clients or any third party of any security breach or privacy breach? (4) Received any cyber extortion demand or threat? (5) Sustained any unscheduled network outage or interruption for any reason? (6) Sustained any property damage or business interruption losses as a result of a cyber-attack? (7) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud?		☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
b. Do you or any other person or organization proposed for this insurance have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim?		☐ Yes ☐ No
c. In the past 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 4 hours? If "Yes", did the Applicant experience an interruption in business as a result of such outage or interruption?		☐ Yes ☐ No ☐ Yes ☐ 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 questions 9.a. through 9.c. 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 NetGuard® Plus 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