

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.

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:

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. 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</u> Fiscal Year ending / (current projected)	<u>Last</u> Fiscal Year ending /	<u>Two</u> 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? ☐ Yes ☐ No

If "Yes", provide the approximate number of unique records:

Paper records: _____ Electronic records: _____

*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. 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? ☐ Yes ☐ No

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

c. Do you process, store, or handle credit card transactions? ☐ Yes ☐ No
If "Yes", are you PCI-DSS Compliant? ☐ Yes ☐ No

5. 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.

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

Name:

Title:

Phone:

Email address:

IT Security Designation(s):

b. The Applicant's network security is: ☐ Outsourced; provide the name of your network security provider: _____

☐ Managed internally/in-house

c. If the Applicant's network security is outsourced, are you the main contact for the network security provider named in question b. above? ☐ Yes ☐ No

If "No", provide the name and email address for the main contact: _____

d. How many IT personnel are on your team?

e. How many dedicated IT security personnel are on your team?

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 1) the Insurer conducting non-intrusive scans of your internet-facing systems / applications for common vulnerabilities, 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.

Print/Type Name: _____

Signature: _____

6. INFORMATION AND NETWORK SECURITY CONTROLS

a. Do you use a cloud provider to store data or host applications? ☐ Yes ☐ No

If "Yes", provide the name of the cloud provider: _____

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.

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

c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? ☐ Yes ☐ No

If "No", are the following compensating controls in place:

(1) Segregation of servers that store sensitive and confidential information? ☐ Yes ☐ No

(2) Access control with role-based assignments? ☐ Yes ☐ No

7. RANSOMWARE CONTROLS

a. Do you pre-screen emails for potentially malicious attachments and links? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Select your email security provider:

If "Other", provide the name of your email security provider: _____

(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? ☐ Yes ☐ No

b. Can your users access email through a web application or a non-corporate device? ☐ Yes ☐ No

If "Yes", do you enforce **MFA**? ☐ Yes ☐ No

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

If "Yes", do you use **MFA** to secure all remote access to your network, including any **remote desktop protocol (RDP)** connections? ☐ Yes ☐ No

If **MFA** is used, complete the following:

(1) Select your **MFA** provider:

If "Other", provide the name of your **MFA** provider: _____

(2) Select your **MFA** type:

If "Other", describe your **MFA** type: _____

(3) Does your **MFA** configuration ensure that the compromise of a single device will only compromise a single authenticator? ☐ Yes ☐ No

d. Do you use a **next-generation antivirus (NGAV)** product to protect all endpoints across your enterprise? ☐ Yes ☐ No

If "Yes", select your **NGAV** provider:

If "Other", provide the name of your **NGAV** provider: _____

e. Do you use an **endpoint detection and response (EDR)** tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Select your **EDR** provider:

If "Other", provide the name of your **EDR** provider: _____

(2) Do you enforce application whitelisting/blacklisting? ☐ Yes ☐ No

	(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.	<input type="checkbox"/> Yes <input type="checkbox"/> No
	(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?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
f.	Do you use MFA to protect all local and remote access to privileged user accounts? If "Yes", select your MFA type: If "Other", describe your MFA type: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No
g.	Do you use a data backup solution? If "Yes":	<input type="checkbox"/> Yes <input type="checkbox"/> No
	(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 (describe your data backup solution): _____	
	(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.	
	(3) How frequently are backups run? <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Monthly	
	(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	
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?	<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.	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. 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? ☐ Yes ☐ No
 - (2) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? ☐ Yes ☐ No
 - (3) Notified customers, clients or any third party of any security breach or privacy breach? ☐ Yes ☐ No
 - (4) Received any cyber extortion demand or threat? ☐ Yes ☐ No
 - (5) Sustained any unscheduled network outage or interruption for any reason? ☐ Yes ☐ No
 - (6) Sustained any property damage or business interruption losses as a result of a cyber-attack? ☐ Yes ☐ No
 - (7) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? ☐ 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? ☐ Yes ☐ No
- If "Yes", did the Applicant experience an interruption in business as a result of such outage or interruption? ☐ 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, 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 NetGuard® Plus 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