

Cyber & Professional Lines Group

16501 Ventura Blvd. Suite 200, Encino, CA 91436 main (818) 382-2030

NetGuard® Plus Cyber Liability Insurance Renewal 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	ie:			
Website:						Fax:				
Primary Contact Name:					!	Prima	ary Contact E-Mail:			
Applicant is a(an):			☐ Indiv	vidual 🗌 Corporation 🔲 Par	tnership		Other:		_	
2.	RE	QUIRED ADDITIONAL INFORMATION								
	a.	Total number o	f employees:							
	b.	months?	he name of the Applicant changed, or has any merger or consolidation taken place, in the past 12 ns? s", please provide details on a separate page.						☐ Yes ☐ No	
	c.	Have there bee	n any m	naterial changes in the Applicant's se	ecurity co	ontrol	ls in the past 12 mo	nths?	☐ Yes ☐ No	
		If "Yes", please provide details on a separate page.								
	d.	Has the Applicant acquired any subsidiaries, affiliated companies or entities in the past 12 months?							☐ Yes ☐ No	
	If "Yes", please attach a list with 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.	RE	VENUES								
				Current Fiscal Year			La	ast Fiscal Year		
				ending /				ending /		
				(current projected)						
Tota	al gro	ss revenues:		\$		\$	\$			
4.	RE	CORDS								
	a.	or electronic for	rm?	ost, process, control, use or share a				n* in either paper	☐ Yes ☐ No	
		=	-	de the approximate number of uni	-					
		Paper records			tronic re			signaly identify a		
		person, includi payment card	*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.	fingerprints, voi characteristics	you collect, store, host, process, control, use or share any biometric information or data, such as gerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral aracteristics 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		
5.	INF	INFORMATION AND NETWORK SECURITY CONTROLS								
	a.	Do you use ant	anti-virus software and a firewall to protect your network?					☐ Yes ☐ No		
	b.	Do you use a cloud provider to store data or host applications?						☐ Yes ☐ No		
		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., medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.								

NGP-RNA (10.2020) Page 1 of 3

	c.	Do you use 2-factor authentication to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)?					
	d.	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?	☐ Yes ☐ No				
		(2) Access control with role-based assignments?	Yes No				
	e.	Do you process, store, or handle credit card transactions?	☐ Yes ☐ No				
		If "Yes", are you PCI-DSS Compliant?	☐ Yes ☐ No				
6.	RA	NSOMWARE CONTROLS					
	a.	Do you allow remote access to your network? If "Yes":	☐ Yes ☐ No				
		(1) Do you use 2-factor authentication to secure all remote access to your network?	☐ Yes ☐ No				
		(2) Do you utilize IP whitelisting to further protect remote access connections?	☐ Yes ☐ No				
	b.	Have you disabled the Remote Desktop Protocol (RDP) and/or Remote Desktop Gateway (RDG) on all					
		system endpoints and servers?	☐ Yes ☐ No				
		If "No", is RDP and/or RDG protected by two-factor authentication?	☐ Yes ☐ No				
	c.	Do you use 2-factor authentication to secure all domain or network administrator accounts?	☐ Yes ☐ No				
	d.	Do you use 2-factor authentication to secure remote access to your email accounts?	☐ Yes ☐ No				
	e.	Do you use Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) software (e.g.,					
		CrowdStrike, Cylance, Carbon Black) to secure all system endpoints?	☐ Yes ☐ No				
		If "Yes", please list your provider:					
	f.	Do you use an email filtering solution designed to prevent phishing or ransomware attacks (in addition to any					
		filtering solution(s) provided by your email provider)? If "Yes", please provide the name of your filtering solution provider:	☐ Yes ☐ No				
		Do you use a data backup solution for all critical data?	☐ Yes ☐ No				
	g.	If "Yes":	☐ Yes ☐ No				
		(1) How frequently does it run? Daily Weekly Monthly					
		(2) Which of the following best describes your data backup solution?					
		☐ Local backup					
		☐ Network drive					
		☐ Tape backup					
		 ☐ Off-site storage ☐ Cloud backup 					
		☐ Other:					
		(3) Please list your data backup provider:					
		(4) Is your data backup solution:					
		(a) physically disconnected from your network?	☐ Yes ☐ No				
		(b) segregated with 2-factor authentication access control?	☐ Yes ☐ No				
		(5) How long do you expect it to take to recover from backups 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					
7.	PH	SHING CONTROLS					
	a.	Do all employees with financial or accounting responsibilities at your company complete social engineering					
		training?	☐ Yes ☐ No				
	<u>_</u>	If "Yes", does such training include phishing simulation? Does your organization send and/or receive wire transfers?	Yes No				
	b.	If "Yes", does your wire transfer authorization process include the following:	☐ Yes ☐ No				
		(1) A wire request documentation form?	☐ Yes ☐ No				
		(2) A protocol for obtaining proper written authorization for wire transfers?	☐ Yes ☐ No				
		(3) A separation of authority protocol?	☐ Yes ☐ 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?					
		(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 before the change request was received?	□ Yes □ No				

NGP-RNA (10.2020) Page **2** of **3**

8. LOSS HISTORY										
If the answer to question 8.a. or 8.b. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.										
 a. In the past 12 months, has the Applicant or any other per (1) Received any complaints or written demands or been injury, breach of private information, network secur denial of service attacks, computer virus infections, or the ability of third parties to rely on the Applicant's (2) Been the subject of any government action, invest violation of privacy law or regulation? (3) Notified customers, clients or any third party of any set (4) Received any cyber extortion demand or threat? (5) Sustained any unscheduled network outage or interrupt (6) Sustained any property damage or business interrupt (7) Sustained any losses due to wire transfer fraud, tele b. In the past 12 months, has any IT service provider that network outage or interruption lasting longer than 4 hours. 	en a subject in litigation involving matters of privacy ty, defamation, content infringement, identity theft, theft of information, damage to third party networks network? gation or other proceedings regarding any alleged ecurity breach or privacy breach? uption for any reason? tion losses as a result of a cyber-attack? communications fraud or phishing fraud? the Applicant relies on sustained an unscheduled									
If "Yes", did the Applicant experience an interruption		☐ Yes ☐ No								
received, in the past 12 months? If "No", please forward complete details to Tokio Man	3,									
NOTICE TO APPLICANT										
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									

NGP-RNA (10.2020) Page **3** of **3**