

NetGuard[®] Plus Cyber Liability Insurance 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:				
Prim	ary (Contact Name:					Primary Co	ntact E-Ma	il:	
2.	FO	RM OF BUSINESS								
	a. Applicant is a(an):									
	b. Date established:									
	c.	Description of operation	ons:							
	d.	Total number of emplo	oyees:							
		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.	RE	VENUES	1							
			Current Fiscal Year		La	Last Fiscal Year		Two Fiscal Years ago		
				ending	/		ending /		ending	/
				(current pro	ojected)					
Tot		oss revenues:	\$			\$			\$	
4.		CORDS								
	a.	Do you collect, store or electronic form?	, host, p	process, con	trol, use or sl	nare any priv	ate or sensiti	ve informat	ion* in either paper	🗌 Yes 🗌 No
		If "Yes", please pro				-				
		·					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	
5.	INFORMATION AND NETWORK SECURITY CONTROLS								1	
	a.	Do you use anti-virus	Do you use anti-virus software and a firewall to protect your network?						🗌 Yes 🗌 No	
	b.	Do you use a cloud p	o 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., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.								
	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)?						🗌 Yes 🗌 No		

	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			
	е.	Do you process, store, or handle credit card transactions?	🗌 Yes 🗌 No			
		If "Yes", are you PCI-DSS Compliant?	🗌 Yes 🗌 No			
6.	RA	NSOMWARE CONTROLS	1			
	a.	Do you allow remote access to your network?	🗌 Yes 🗌 No			
		lf "Yes":				
		(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.					
		system endpoints and servers?				
		If "No", is RDP and/or RDG protected by two-factor authentication?	Yes No			
	с.	Do you use 2-factor authentication to secure all domain or network administrator accounts?				
	d.	Do you use 2-factor authentication to secure remote access to your email accounts?	🗌 Yes 🗌 No			
	е.	Do you use Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) software (e.g.,	🗌 Yes 🗌 No			
		CrowdStrike, Cylance, Carbon Black) to secure all system endpoints?				
		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)?	🗌 Yes 🗌 No			
		If "Yes", please provide the name of your filtering solution provider:				
	g.	Do you use a data backup solution for all critical data?	🗌 Yes 🗌 No			
		If "Yes":				
		(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?				
7						
7.		ISHING CONTROLS				
	а.	Do any of the following employees at your company complete social engineering training:				
		 (1) Employees <u>with</u> financial or accounting responsibilities? (2) Enclose the second se	🗌 Yes 🗌 No			
		(2) Employees <u>without</u> financial or accounting responsibilities?	🗌 Yes 🗌 No			
		If "Yes" to question 7.a.(1) or 7.a.(2) above, does your social engineering training include phishing simulation?	🗌 Yes 🗌 No			
	b					
	b.	Does your organization send and/or receive wire transfers?	🗌 Yes 🗌 No			
		If "Yes", does your wire transfer authorization process include the following:				
		(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?	🗌 Yes 🗌 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	🗌 Yes 🗌 No			
1		vendor, client or customer <u>before</u> the change request was received?				

8.	8. LOSS HISTORY								
	If the answer to any question in 8.a. through 8.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.								
	a.		he past 3 years, has the Applicant or any other person Received any complaints or written demands or been injury, breach of private information, network security denial of service attacks, computer virus infections, th or the ability of third parties to rely on the Applicant's	a subject in litigation involving matters of privacy , defamation, content infringement, identity theft, neft of information, damage to third party networks	🗌 Yes 🗌 No				
		(2)	Been the subject of any government action, investiga violation of privacy law or regulation?	tion or other proceedings regarding any alleged	Yes No				
		(3)	Notified customers, clients or any third party of any se	ecurity breach or privacy breach?					
			Received any cyber extortion demand or threat?	, , ,	☐ Yes ☐ No ☐ Yes ☐ No				
			Sustained any unscheduled network outage or interru	ption for any reason?					
		(6)	Sustained any property damage or business interrupt						
		(7)	Sustained any losses due to wire transfer fraud, telec	•					
	b.	bre	you or any other person or organization proposed for ach, privacy breach, privacy-related event or incident of a claim?	or this insurance have knowledge of any security	 Yes No				
	C.		he past 3 years, has any service provider with access tained an unscheduled network outage or interruption		🗌 Yes 🗌 No				
			Yes", did the Applicant experience an interruption?	on in business as a result of such outage or	🗌 Yes 🗌 No				
NOT	ICE	TO A	APPLICANT						
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 8.a. through 8.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.									
CER	TIFI	CATI	ON 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.									
be s date	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.									
Prin	t or T	Гуре	Applicant's Name	Title of Applicant					
Signature of Applicant D				Date Signed by Applicant					
L									