TOKIO MARINE HCC
16501 Ventura Blvd. Suite 200 Encino, CA 91436
tmhcc.com/pro

Florida Lawyers Mutual Insurance Company
NetGuard® Plus Cyber Liability Insurance Increased Limits Program

Law firms regularly maintain vast amounts of sensitive data, including personal and corporate information of clients, employees, and even parties and witnesses in litigation. Should a data breach occur, law firms can be exposed to claims for liability, reputational harm, and significant losses in complying with breach notification laws. Tokio Marine HCC - Cyber & Professional Lines Group ("TMHCC - CPLG") now offers a streamlined application process and simplified underwriting for Florida Lawyers Mutual Insurance Company ("FLMIC") policyholders who meet the NetGuard® Plus Cyber Liability Insurance program qualifications. Qualified Applicants can simply complete the Program Application, choose a limit, request to bind coverage and pay the applicable premium.

THIRD PARTY LIABILITY COVERAGE COMPONENTS

- **Multimedia Liability Coverage** – Coverage for defense costs and damages incurred in claims alleging liability resulting from the dissemination of online or offline multimedia material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.
- **Security and Privacy Liability Coverage** – Coverage for defense costs and damages incurred in claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information or failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from an insured computer system to the computer system of a third party.
- **Privacy Regulatory Defense and Penalties Coverage** - Coverage for defense costs and regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, local or foreign governmental agencies.
- **PCI DSS Liability Coverage** – Coverage for defense costs and assessments, fines and penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.
- **Bodily Injury Liability Coverage** - Coverage for defense costs and damages incurred in claims alleging liability for bodily injury caused by a security breach or privacy breach.
- **Property Damage Liability Coverage** - Coverage for defense costs and damages incurred in claims alleging liability for failure to prevent or avoid property damage caused by a security breach or privacy breach.
- **TCPA Defense Coverage** – Defense-only coverage for claims alleging violation of the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the CAN-Spam Act, or any similar federal, state, local or foreign law regulating the use of telephonic or electronic communications for solicitation purposes.

FIRST PARTY COVERAGE COMPONENTS

- **Breach Event Costs Coverage** – Coverage for reasonable and necessary mitigation costs and expenses incurred as a result of a privacy breach, security breach or adverse media report, such as legal expenses, public relations expenses, IT forensic expenses, breach notification costs (including voluntary notification costs), and the cost to set up call centers and provide credit monitoring and identity theft assistance.
- **Post Breach Remediation Costs Coverage** – Coverage for post-breach remediation costs incurred to mitigate the potential of a future security breach or privacy breach.

- **BrandGuard® Coverage** - Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach. **A 2-week waiting period and 6-month period of indemnity apply to BrandGuard® coverage.**
- **System Failure Coverage** – Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and business income loss and interruption expenses incurred, due to an unplanned outage, interruption, failure, suspension, or degradation of service of an insured computer system, including any such incident caused by a hacking attack. **An 8-hour waiting period and 6-month period of restoration apply to the business interruption coverage component of System Failure.**
- **Dependent System Failure Coverage** – Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and business income loss and extra expenses incurred, due to an unplanned outage, interruption, failure, suspension, or degradation of service of an IT service provider computer system that is caused by specified cyber perils, including a denial of service attack, malicious code and acts of cyber terrorism. **A 12-hour waiting period and 4-month period of indemnity apply to the business interruption coverage component of Dependent System Failure.**
- **Cyber Extortion Coverage** – Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.
- **Cyber Crime Coverage**
  - (1) **Financial Fraud** – Coverage for your loss of money or securities due to financial fraud, including wire transfer fraud;
  - (2) **Telecommunications and Utilities Fraud** – Coverage for (1) charges you incur for unauthorized calls resulting from the fraudulent use of an insured telephone system and (2) losses resulting from the fraudulent use of utilities, such as electricity, water, internet access and cloud computing; and
  - (3) **Phishing Fraud**
    - a) **Your Phishing Fraud Loss** – Coverage for your loss of money, securities or other property due to phishing schemes that trick an Insured to transfer, pay or deliver money, securities or other property to an unintended third party, plus expenses incurred to notify your clients or customers of such phishing fraud.
    - b) **Client Phishing Fraud Loss** – Coverage for your loss of money, securities or other property which your client, customer or vendor intended to pay to you, but which was paid to an unintended third party due to a phishing scheme that tricked your client, customer or vendor by impersonating an Insured, plus the cost of reimbursing your customers, clients or vendors for their own losses that result from such phishing schemes.
- **Bricking Loss Coverage** – Coverage for the costs incurred to replace computer hardware or electronic equipment that has been rendered nonfunctional due to a hacking attack, up to 125% of replacement value.
- **Property Damage Loss Coverage** – Coverage for damage to your property resulting from a hacking attack.
- **Reward Expenses Coverage** – Coverage for reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, or phishing attack.
- **Court Attendance Costs Coverage** – Coverage for reasonable costs incurred to attend court, arbitration, mediation, or other legal proceedings or hearings as a witness in a claim covered under the policy.

PROGRAM HIGHLIGHTS

- Full unknown prior acts coverage
- Separate Breach Event Costs Limit Enhancement and Additional Defense Costs Limit are included
- Aggregate Deductible provides a maximum Deductible amount the Insured will be obligated to pay during the policy period; will be 3x the “each Claim” Deductible amount
- Broad coverage for data that is stored with third parties, including outsourced IT providers, BPO service providers and independent contractors
- Worldwide coverage, where permissible
- Coverage for proactive breach response costs and voluntary notification is provided up to the full limit
- Covers the cost of providing 24 months of credit, identity or healthcare record monitoring services, fraud alerts, identity theft assistance services, or credit or identity repair and restoration services
- System Failure Coverage applies to voluntary shutdowns
- Property Damage exclusion does not apply to electronic data
- Coverage applies to breach of corporate information
- Coverage applies to acts committed by rogue employees, as well as privacy claims brought by employees
- Multimedia Liability Coverage and Security & Privacy Liability Coverage apply to liability assumed under contract
- Extended Reporting Period available for 1-3 years
- Access to risk management services

PROGRAM QUALIFICATIONS

- Applicant **must** be insured with FLMIC for lawyers’ Professional Liability Insurance;
- Applicant **must** be a law firm with maximum annual revenues of $20,000,000;
- Applicant **must not** have experienced any related claims/incidents in the last 3 years;
- Applicant **must not** handle real estate and/or title transactions; and
- Applicant’s application responses **must** meet our program requirements.

If you do not meet the program qualifications, coverage cannot be bound under this program; however, you can still be considered for coverage outside the program. To be considered for coverage outside this program, please complete the enclosed application and submit it to your agent.

INELIGIBLE PRACTICE AREAS

Real estate lawyers or law firms with real estate law practice areas are not eligible for this program; however, such Applicants can be referred to Tokio Marine HCC for coverage outside of the program, subject to individual underwriting.

$250,000 AGGREGATE LIMIT

The Additional Defense Costs Limit and Breach Event Costs Limit are in addition to the Maximum Policy Aggregate Limit.

Coverage	Limits	Deductible
Multimedia Liability Coverage	$250,000 **each Claim/aggregate**	$0 **each Claim**
Security and Privacy Liability Coverage	$250,000 **each Claim/aggregate**	$0 **each Claim**
Privacy Regulatory Defense and Penalties Coverage	$250,000 **each Claim/aggregate**	$0 **each Claim**
PCI DSS Liability Coverage	$250,000 **each Claim/aggregate**	$0 **each Claim**
Bodily Injury Liability Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
Property Damage Liability Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
TCPA Defense Coverage	$10,000 **each Claim/aggregate**	$2,500 **each Claim**
Breach Event Costs Coverage	$250,000 **each Claim/aggregate**	$0 **each Claim**
Post Breach Remediation Costs Coverage	$5,000 **each Claim/aggregate**	$2,500 **each Claim**
BrandGuard® Coverage **Waiting Period: 2 weeks** **Period of Indemnity: 6 months**	$250,000 **each Claim/aggregate**	N/A
System Failure Coverage **Business Interruption Waiting Period**: **8 hours** **Period of Restoration: 6 months**	$250,000 **each Claim/aggregate**	$0 **each Claim**
Dependent System Failure Coverage **Business Interruption Waiting Period: 12 hours** **Period of Indemnity: 4 months**	$250,000 **each Claim/aggregate**	$0 **each Claim**
Cyber Extortion Coverage	$250,000 **each Claim/aggregate**	$0 **each Claim**
Cyber Crime Coverage	$25,000 **aggregate**	$2,500 **each Claim**
A. Financial Fraud Sublimit	$25,000 **each Claim/aggregate**	
B. Telecommunications Fraud Sublimit	$25,000 **each Claim/aggregate**	
C. Phishing Fraud Aggregate Sublimit **(for C.1. and C.2.)**	$25,000 **aggregate**	
1. Your Phishing Fraud Loss Sublimit	$25,000 **each Claim/aggregate**	
2. Client Phishing Fraud Loss Sublimit	$10,000 **each Claim/aggregate**	
Bricking Loss Coverage	$250,000 **each Claim/aggregate**	$2,500 **each Claim**
Property Damage Loss Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
Reward Expenses Coverage	$10,000 **each Claim/aggregate**	$2,500 **each Claim**
Court Attendance Costs Coverage	$5,000 **each Claim/aggregate**	None

Additional Defense Costs Limit	$250,000 aggregate
Separate Breach Event Costs Limit Enhancement	Included
Aggregate Deductible	$7,500
Maximum Policy Aggregate Limit	$250,000

RATES FOR $250K LIMIT OPTION
(valid through 12/31/2021)

Revenue	Annual Premium
<$500,000 - $4,000,000	$450
$4,000,001 - $5,000,000	$539
$5,000,001 - $6,000,000	$660
$6,000,001 - $7,000,000	$779
$7,000,001 - $8,000,000	$900
$8,000,001 - $9,000,000	$1,030
$9,000,001 - $10,000,000	$1,104
$10,000,001 - $11,000,000	$1,135
$11,000,001 - $12,000,000	$1,166
$12,000,001 - $13,000,000	$1,197
$13,000,001 - $14,000,000	$1,228
$14,000,001 - $15,000,000	$1,259
$15,000,001 - $16,000,000	$1,281
$16,000,001 - $17,000,000	$1,302
$17,000,001 - $18,000,000	$1,323
$18,000,001 - $19,000,000	$1,344
$19,000,001 - $20,000,000	$1,366
$20,000,001+	Refer to TMHCC - CPLG

$500,000 AGGREGATE LIMIT

The Additional Defense Costs Limit and Breach Event Costs Limit are in addition to the Maximum Policy Aggregate Limit.

Coverage	Limits	Deductible
Multimedia Liability Coverage	$500,000 **each Claim/aggregate**	$0 **each Claim**
Security and Privacy Liability Coverage	$500,000 **each Claim/aggregate**	$0 **each Claim**
Privacy Regulatory Defense and Penalties Coverage	$500,000 **each Claim/aggregate**	$0 **each Claim**
PCI DSS Liability Coverage	$500,000 **each Claim/aggregate**	$0 **each Claim**
Bodily Injury Liability Coverage	$100,000 **each Claim/aggregate**	$2,500 **each Claim**
Property Damage Liability Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
TCPA Defense Coverage	$25,000 **each Claim/aggregate**	$2,500 **each Claim**
Breach Event Costs Coverage	$500,000 **each Claim/aggregate**	$0 **each Claim**
Post Breach Remediation Costs Coverage	$10,000 **each Claim/aggregate**	$2,500 **each Claim**
BrandGuard® Coverage **Waiting Period: 2 weeks** **Period of Indemnity: 6 months**	$500,000 **each Claim/aggregate**	N/A
System Failure Coverage **Business Interruption Waiting Period**: **8 hours** **Period of Restoration: 6 months**	$500,000 **each Claim/aggregate**	$0 **each Claim**
Dependent System Failure Coverage **Business Interruption Waiting Period: 12 hours** **Period of Indemnity: 4 months**	$500,000 **each Claim/aggregate**	$0 **each Claim**
Cyber Extortion Coverage	$500,000 **each Claim/aggregate**	$0 **each Claim**
Cyber Crime Coverage	$50,000 **aggregate**	$2,500 **each Claim**
A. Financial Fraud Sublimit	$50,000 **each Claim/aggregate**	
B. Telecommunications Fraud Sublimit	$50,000 **each Claim/aggregate**	
C. Phishing Fraud Aggregate Sublimit **(for C.1. and C.2.)**	$50,000 **aggregate**	
1. Your Phishing Fraud Loss Sublimit	$50,000 **each Claim/aggregate**	
2. Client Phishing Fraud Loss Sublimit	$25,000 **each Claim/aggregate**	
Bricking Loss Coverage	$500,000 **each Claim/aggregate**	$2,500 **each Claim**
Property Damage Loss Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
Reward Expenses Coverage	$25,000 **each Claim/aggregate**	$2,500 **each Claim**
Court Attendance Costs Coverage	$10,000 **each Claim/aggregate**	None

Additional Defense Costs Limit	$500,000 aggregate
Separate Breach Event Costs Limit Enhancement	Included
Aggregate Deductible	$7,500
Maximum Policy Aggregate Limit	$500,000

RATES FOR $500K LIMIT OPTION
(valid through 12/31/2021)

Revenue	Annual Premium
<$500,000 - $3,000,000	$500
$3,000,001 - $4,000,000	$546
$4,000,001 - $5,000,000	$701
$5,000,001 - $6,000,000	$858
$6,000,001 - $7,000,000	$1,013
$7,000,001 - $8,000,000	$1,170
$8,000,001 - $9,000,000	$1,339
$9,000,001 - $10,000,000	$1,435
$10,000,001 - $11,000,000	$1,475
$11,000,001 - $12,000,000	$1,516
$12,000,001 - $13,000,000	$1,556
$13,000,001 - $14,000,000	$1,597
$14,000,001 - $15,000,000	$1,637
$15,000,001 - $16,000,000	$1,665
$16,000,001 - $17,000,000	$1,693
$17,000,001 - $18,000,000	$1,720
$18,000,001 - $19,000,000	$1,748
$19,000,001 - $20,000,000	$1,775
$20,000,001+	Refer to TMHCC - CPLG

$1M AGGREGATE LIMIT

The Additional Defense Costs Limit and Breach Event Costs Limit are in addition to the Maximum Policy Aggregate Limit.

Coverage	Limits	Deductible
Multimedia Liability Coverage	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Security and Privacy Liability Coverage	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Privacy Regulatory Defense and Penalties Coverage	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
PCI DSS Liability Coverage	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Bodily Injury Liability Coverage	$250,000 **each Claim/aggregate**	$2,500 **each Claim**
Property Damage Liability Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
TCPA Defense Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
Breach Event Costs Coverage	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Post Breach Remediation Costs Coverage	$25,000 **each Claim/aggregate**	$2,500 **each Claim**
BrandGuard® Coverage **Waiting Period: 2 weeks** **Period of Indemnity: 6 months**	$1,000,000 **each Claim/aggregate**	N/A
System Failure Coverage **Business Interruption Waiting Period**: **8 hours** **Period of Restoration: 6 months**	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Dependent System Failure Coverage **Business Interruption Waiting Period: 12 hours** **Period of Indemnity: 4 months**	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Cyber Extortion Coverage	$1,000,000 **each Claim/aggregate**	$0 **each Claim**
Cyber Crime Coverage	$100,000 **aggregate**	$2,500 **each Claim**
A. Financial Fraud Sublimit	$100,000 **each Claim/aggregate**	
B. Telecommunications Fraud Sublimit	$100,000 **each Claim/aggregate**	
C. Phishing Fraud Aggregate Sublimit **(for C.1. and C.2.)**	$100,000 **aggregate**	
1. Your Phishing Fraud Loss Sublimit	$100,000 **each Claim/aggregate**	
2. Client Phishing Fraud Loss Sublimit	$50,000 **each Claim/aggregate**	
Bricking Loss Coverage	$1,000,000 **each Claim/aggregate**	$2,500 **each Claim**
Property Damage Loss Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
Reward Expenses Coverage	$50,000 **each Claim/aggregate**	$2,500 **each Claim**
Court Attendance Costs Coverage	$25,000 **each Claim/aggregate**	None

Additional Defense Costs Limit	$1,000,000 aggregate
Separate Breach Event Costs Limit Enhancement	Included
Aggregate Deductible	$7,500
Maximum Policy Aggregate Limit	$1,000,000

RATES FOR $1M LIMIT OPTION
(valid through 12/31/2021)

Revenue	Annual Premium
<$500,000 - $3,000,000	$653
$3,000,001 - $4,000,000	$840
$4,000,001 - $5,000,000	$1,079
$5,000,001 - $6,000,000	$1,320
$6,000,001 - $7,000,000	$1,559
$7,000,001 - $8,000,000	$1,799
$8,000,001 - $9,000,000	$2,061
$9,000,001 - $10,000,000	$2,208
$10,000,001 - $11,000,000	$2,270
$11,000,001 - $12,000,000	$2,332
$12,000,001 - $13,000,000	$2,394
$13,000,001 - $14,000,000	$2,457
$14,000,001 - $15,000,000	$2,518
$15,000,001 - $16,000,000	$2,561
$16,000,001 - $17,000,000	$2,604
$17,000,001 - $18,000,000	$2,646
$18,000,001 - $19,000,000	$2,689
$19,000,001 - $20,000,000	$2,731
$20,000,001+	Refer to TMHCC - CPLG

POLICY & ENDORSEMENTS LINKS

This Policy is underwritten by TMHCC – CPLG on our Houston Casualty Company NetGuard® Plus Cyber Liability Insurance Policy (NGP 1000 (4.2020)) and endorsed with:

- Service of Suit NGP 1075 (4.2020)
- Policyholder Disclosure Notice of Terrorism Insurance Coverage NGP 1076 (4.2020)
- Nuclear Incident Exclusion NGP 1078 (5.2020)
- Amendment of Other Insurance Provisions: Excess Insurance Endorsement NGP 1082 (5.2020)

HOW TO PURCHASE THIS INSURANCE

1. Fully complete the attached NetGuard® Plus Cyber Liability Insurance Program Application.
2. Calculate the applicable premium from the rate chart.
3. Sign and date (must be within 60 days prior to binding) and return the completed Application to your broker with your check for the premium, plus state taxes, policy issuance fee and any applicable broker fee.

Cyber & Professional Lines Group
16501 Ventura Blvd. Suite 200, Encino, CA 91436
main (818) 382-2030

NetGuard® Plus Cyber Liability Insurance Program 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		Phone	
City, State, Zip		Fax	
Website		Contact e-mail	

2. FORM OF BUSINESS			
a. Applicant is a(an): ☐ Individual ☐ Corporation ☐ Partnership ☐ Other: _____			
b. Date established:			
c. Description of operations:			
d. Current professional liability carrier:		Policy number:	
e. Total full-time equivalent professionals:			
f. Total number of employees:			
g. Does the Applicant handle real estate and/or title transactions? **If the answer is "Yes", coverage cannot be bound under this program. However, you can still be considered for coverage outside the program.**			☐ Yes ☐ No
h. 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. COVERAGE DESIRED	
a. Proposed Effective Date:	
b. Retroactive Date:	
c. Limit(s):	
d. Deductible(s):	

5. 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:** _____ ***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.**	☐ 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?	☐ 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

6.	**CLOUD PROVIDER**	
	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.**	☐ Yes ☐ No
7.	**INFORMATION AND NETWORK SECURITY CONTROLS**	
	If the answer to question 7.a. below is "No", coverage cannot be bound under this program. If you desire an indication outside of the program, please provide details for your "No" answer on a separate page.	
a.	Do you use anti-virus software and a firewall to protect your network?	☐ Yes ☐ No
	If the answer to question 7.b. below is "No", you may not qualify for coverage under this program unless you have <u>both</u> compensating controls described in 7.b.(1) and 7.b.(2) in place.	
b.	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:**	☐ Yes ☐ No
	(1) Segregation of servers that store sensitive and confidential information?	☐ Yes ☐ No
	(2) Access control with role-based assignments?	☐ Yes ☐ No
8.	**RANSOMWARE CONTROLS**	
	If the answer to any question in this section is "No", coverage cannot be bound under this program. If you desire an indication outside of the program, please provide details for any "No" answers on a separate page.	
a.	Do you use 2-factor authentication to secure all remote access to your network, including any remote desktop connections?	☐ Yes ☐ No
b.	Do you use 2-factor authentication to secure remote access to your email accounts?	☐ Yes ☐ No
c.	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? **If "Yes", please list your provider:** _____	☐ Yes ☐ No
d.	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
e.	Do you use a data backup solution for all critical data? **If "Yes":**	☐ Yes ☐ No
	(1) How frequently does it run? ☐ Daily ☐ Weekly ☐ Monthly	
	(2) Is your data backup solution segregated and/or disconnected from your network in such a way to reduce or eliminate the risk of the backup being compromised in a malware or ransomware attack that spreads throughout your network?	☐ Yes ☐ No
9.	**PHISHING CONTROLS**	
	If the answer to any question in this section is "No", coverage cannot be bound under this program. If you desire an indication outside of the program, please provide details for any "No" answers on a separate page.	
	Do any of the following employees at your company complete social engineering training:	
	(1) Employees **<u>with</u>** financial or accounting responsibilities?	☐ Yes ☐ No
	(2) Employees **<u>without</u>** financial or accounting responsibilities?	☐ Yes ☐ No
	If "Yes" to question 9.a.(1) or 9.a.(2) above, does your social engineering training include phishing simulation?	☐ Yes ☐ No
10.	**LOSS HISTORY**	
	If the answer to any question in this section is "Yes", coverage cannot be bound under this program. If you desire an indication outside of the program, 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 10.a. through 10.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

POLICYHOLDER DISCLOSURE NOTICE OF TERRORISM INSURANCE COVERAGE

Coverage for acts of terrorism is already included in your policy (including any quotation for insurance) to which this notice applies. You are hereby notified that under the Terrorism Risk Insurance Act, as amended in 2015, the definition of act of terrorism has changed. As defined in Section 102(1) of the Act: The term "act of terrorism" means any act that is certified by the Secretary of the Treasury – in consultation with the Secretary of Homeland Security, and the Attorney General of the United States – to be an act of terrorism; to be a violent act or an act that is dangerous to human life, property or infrastructure; to have resulted in damage within the United States, or outside the United States in the case of certain air carriers or vessels or the premises of a United States mission; and to have been committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion.

Under your coverage, any losses resulting from certified acts of terrorism may be partially reimbursed by the United States Government under a formula established by the Terrorism Risk Insurance Act, as amended. **HOWEVER, YOUR POLICY MAY CONTAIN OTHER EXCLUSIONS WHICH MIGHT AFFECT YOUR COVERAGE, INCLUDING BUT NOT LIMITED TO, AN EXCLUSION FOR NUCLEAR EVENTS. PLEASE READ IT CAREFULLY**. Under the formula, the United States Government generally reimburses 85% through 2015; 84% beginning on January 1, 2016; 83% beginning on January 1, 2017; 82% beginning on January 1, 2018; 81% beginning on January 1, 2019 and 80% beginning on January 1, 2020 of covered terrorism losses exceeding the statutorily established deductible paid by the insurance company providing the coverage. The Terrorism Risk Insurance Act, as amended, contains a USD100 billion cap that limits U.S. Government reimbursement as well as insurers' liability for losses resulting from certified acts of terrorism when the amount of such losses exceeds USD100 billion in any one calendar year. If the aggregate insured losses for all insurers exceed USD100 billion, your coverage may be reduced.

The portion of your annual premium that is attributable to coverage for certified acts of terrorism as defined in the Terrorism Risk Insurance Act, as amended in 2015, is **1%**. This amount does not include any charges for the portion of loss covered by the Federal Government under the Act.

I ACKNOWLEDGE THAT I HAVE BEEN NOTIFIED THAT UNDER THE TERRORISM RISK INSURANCE ACT, AS AMENDED IN 2015, ANY LOSSES CAUSED BY CERTIFIED ACTS OF TERRORISM UNDER MY POLICY MAY BE PARTIALLY REIMBURSED BY THE UNITED STATES GOVERNMENT AND ARE SUBJECT TO A USD100 BILLION CAP THAT MAY REDUCE MY COVERAGE, AND I HAVE BEEN NOTIFIED OF THE PORTION OF MY PREMIUM ATTRIBUTABLE TO SUCH COVERAGE.

INSURANCE CARRIER: Houston Casualty Company