TOKIO MARINE HCC

NetGuard® Plus & MEDEFENSE® Plus 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 & MEDEFENSE® Plus 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 Primary Applicant:

Business Address: Phone:

2. ADDITIONAL ENTITIES / MATERIAL CHANGES

Names of all additional entities seeking coverage under the policy. Include each entity's description of operations and relationship to you, including any percentage of ownership.

Have you acquired any subsidiaries, affiliated companies or entities in the past 12 months? □ Yes □ No

Has your name changed, or has any merger or consolidation taken place, in the past 12 months? □ Yes □ No
If "Yes", provide details on a separate page.

3. WEBSITES / DOMAINS

List all websites/domains owned/operated by all entities seeking coverage:

4. CONFIRMATION OF ENTITIES

This Application is reflective of the total exposure for all entities seeking coverage, both previously existing and any acquired in the past 12 months, including revenues, records, controls, vendors and loss history. □ Yes □ No

5. TOTAL GROSS REVENUES

a. Current Full Fiscal Year:	$
b. Last Completed Fiscal Year:	$

6. RECORDS

a. Do you collect, store, host, process, control, use or share any private or sensitive information, including employee information, in either paper or electronic form? □ Yes □ No
If "Yes", provide the approximate number of unique records in each category:
Basic (name, email, address):
Personally Identifiable Information (PII):
Protected Health Information (PHI):
Payment Card Information:
Total unique records:

b. If "Yes" to question 6.a. above, 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

c. Have you ever, do you currently, or will you ever 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

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

7. BILLING AND COMPLIANCE (Complete Section 7 only if MEDEFENSE® Plus (Regulatory) coverage is desired.)

a. Your annual projected billings: $

b. Has your billing compliance or HIPAA compliance program changed since last year? □ Yes □ No

c. Do you bill all services under the National Provider Identifier (NPI) of the individual who performed the service? □ Yes □ No

If "No', in instances where a mid-level provider's services are billed under a physician's NPI, is that physician present when the services are being rendered? □ Yes □ No

8. INTERNAL SECURITY CONTROLS

a. Do you allow remote access to your network? □ Yes □ No

If "Yes":

(1) Do you use **SSL VPN (Web VPN)** for remote access into your network? □ Yes □ No

(2) Is **Multi-Factor Authentication (MFA)** enforced to secure all remote access to your network for all employees and third parties on all applications, including **VPNs (Virtual Private Network)**, **RDP (Remote Desktop Protocol)**, **RDWeb (Remote Desktop Web)** or any **RMM (Remote Management and Monitoring)** applications? □ Yes □ No

If **MFA** is enforced, 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: ___________________________________

b. 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: ______________________

c. 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) Is **EDR** deployed on 100% of endpoints? □ Yes □ No

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.

d. Do you require **MFA** to protect all local and remote access to privileged user accounts? □ Yes □ No

If "Yes", select your **MFA** type**:**

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

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

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

f. Do you enforce Account Lockout policies for all users? □ Yes □ No

If "Yes", provide the lockout threshold setting: ______________________

9. BACKUP AND RECOVERY POLICIES

Do you use a data backup solution? □ Yes □ No

If "Yes":

a. Which best describes your data backup solution? *Choose an item.*

If "Other", describe your data backup solution: ____

b. Check all that apply:

□ Your backups are encrypted, **immutable** or kept separate from your network **(offline/air-gapped)**.

□ You utilize **MFA** for both internal and external access to your backups.

c. How frequently are backups run?

d. 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?

10. PHISHING CONTROLS

a. Do you require all employees at your company to complete social engineering training that includes phishing simulations? □ Yes □ No

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, a protocol for obtaining proper written authorization for wire transfers, and a separation of authority protocol? □ Yes □ No

(2) 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 before the payment or funds transfer instruction/request was received? □ Yes □ No

(3) 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

11. VENDORS

List your top three (3) most critical vendors and their services and websites/domains.

Name	Services	Websites/Domains

12. REGULATORY LOSS HISTORY (Complete Section 12 only if MEDEFENSE® Plus (Regulatory) coverage is desired.)

a. In the past 12 months, have you, any member of your staff, any other person or entity proposed for this insurance, any consultant, or any person or entity for whom you perform billing services:

(1) had to refund amounts to government (public) and/or commercial (private) payer? □ Yes □ No

i. If "Yes", were refunds greater than or equal to 2% of gross annual billings? □ Yes □ No

ii. If "Yes", were these refunds due to an audit, allegation of improper billing or voluntary self-disclosure? □ Yes □ No

iii. If "No" to **a.(1)ii.** above, were these refund amounts routine in nature? □ Yes □ No

(2) received any billing errors proceeding, demand for restitution or notice of any regulatory investigation, inquiry or action involving actual or potential billing errors or HIPAA, EMTALA or Stark violations? □ Yes □ No

If "Yes" to any question in 12.a. above:

b. Have you notified Tokio Marine HCC of all claims, suits, demands, investigations or inquiries received? □ Yes □ No

If "No", please forward complete details to Tokio Marine HCC immediately.

13. CYBER/PRIVACY LOSS HISTORY

a. In the past 12 months, have you 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 your 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 (excluding weather conditions and routine service interruptions) that lasted longer than 4 hours? □ 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. In the past 12 months, has any service provider that you rely on sustained an unscheduled network outage or interruption that lasted longer than 4 hours? □ Yes □ No

If "Yes", did you experience an interruption in business due to such outage or interruption? □ Yes □ No

If "Yes" to any question in 13.a. or 13.b. above:

c. Have you notified Tokio Marine HCC of all incidents or losses occurring, or claims, suits or demands received? □ Yes □ No

If "No", please forward complete details to Tokio Marine HCC immediately.

14. IT DEPARTMENT

This section must be completed by the individual within your organization who is responsible for network security. In this section, "you" refers only to such individual.

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

Name: Phone:

Title: Email:

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: ______________________________

ADDITIONAL COMMENTS

Use this space to explain any "No" answers in the above sections and/or to list other relevant IT security measures you are utilizing that are not listed above.

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, 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 & MEDEFENSE® Plus 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 common 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

California Fraud Warning

For your protection, California law requires the following to appear on this form: Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

Cyber Glossary

TO ASSIST YOU IN COMPLETING YOUR APPLICATION

Please refer to the terms that apply to your specific application.

Endpoint Detection and Response (EDR) centrally collects and analyzes comprehensive endpoint data across your entire organization to provide a full picture of potential threats.

Common Providers: Carbon Black Cloud; Crowdstrike Falcon Insight; SentinelOne; Windows Defender Endpoint

Immutable backups are backup files that are fixed and unchangeable, allowing immediate deployment in the event of ransomware attacks or other data loss.

Multi-Factor Authentication (MFA) is an electronic authentication requiring two or more forms of verification, such as knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print).

Common MFA providers for remote network access: Okta; Duo; LastPass; OneLogin; and Auth0.

Next-Generation Anti-Virus (NGAV) is endpoint antivirus software that leverages predictive analytics driven by machine learning and artificial intelligence with threat intelligence to detect and prevent malware and fileless non-malware attacks, identify malicious behavior, and respond to new and emerging threats that previously went undetected.

Common Providers: BitDefender™; Carbon Black; CrowdStrike Falcon Prevent; SentinelOne; Sophos; Symantec

Offline/Air-gapped backup solution is a backup and recovery solution in which your data is stored offline (i.e., disconnected) and cannot be accessed. If a file or system of files has no connection to the internet or a LAN, it can't be remotely hacked or corrupted.

Personally Identifiable Information (PII) is information that can be used to determine, distinguish or trace an individual's identity, including, but is not limited to, financial account numbers, security codes, personal identification numbers (PINs), credit and debit card numbers, social security numbers, driver's license numbers, addresses, passwords, and any other non-public information as defined in the policy form.

Protected Health Information (PHI) is health-related information that can identify an individual, including demographic identifiers in medical records (names, phone numbers, emails, and biometric information like fingerprints, voiceprints, genetic information, and facial images).

Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol enabling users to connect remotely to another computer via a graphical interface. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Remote Desktop Web (RDWeb), also known as Microsoft Remote Desktop Web Access, is a service that provides remote access to corporate resources through a web portal, including remote desktop access and other applications published on the portal.

Remote Monitoring and Management (RMM) tools allow IT providers to remotely manage and monitor network environments, including remote access, patch management, and reporting functionalities.

Common Providers: ConnectWise and ManageEngine

SSL VPN (Web VPN) simplifies user authentication and network connection by allowing users to login over a webpage from any device, managed or unmanaged, without installing client software. While convenient, it is easily discoverable by threat actors.

Common Providers: Fortnet, Cisco, and Palo Alto VPN Appliances

Virtual Private Network (VPN) encrypts connections between a remote device and an internal network, securing external access to internal systems.

Common Providers: Fortnet, Cisco, and Palo Alto VPN Appliances