TOKIO MARINE HCC

NetGuard® Plus & MEDEFENSE® Plus Insurance

ONLINE 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:

Website **(List all websites/domains owned/operated by all entities seeking coverage)**:

Attach a list of all subsidiaries, affiliated companies or entities owned by you and include a description of (1) the nature of operations of each such subsidiary, affiliated company or entity; (2) its relationship to you; and (3) your percentage of ownership.

2. ADDITIONAL ENTITIES / MATERIAL CHANGES

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. TOTAL GROSS REVENUES

Current Full Fiscal Year: $

4. RECORDS

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 and electronic):

5. BILLING AND COMPLIANCE (Complete Section 5 only if MEDEFENSE® Plus (Regulatory) coverage is desired.)

Does your practice meet both compliance standards:
(1) Complies with HIPAA regulations; and
(2) Either:
- Has a billing compliance program in place using a current edition of the CPT manual; or
- Outsources all billing to a third-party billing company?

☐ Yes ☐ No

6. RANSOMWARE CONTROLS

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

If "Yes", 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

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", select your **EDR** provider:

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

7. REGULATORY LOSS HISTORY (Complete Section 7 only if MEDEFENSE® Plus (Regulatory) coverage is desired.)

If the answer to any question below is "Yes", please provide details for each claim, allegation or incident.

a. After internal inquiry, 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:
- had to refund amounts to government (public) and/or commercial (private) payers within the past 12 months?
- 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

b. Have you notified Tokio Marine HCC of all claims, suits, demands, investigations or inquiries received in the past 12 months? ☐ Yes ☐ No ☐ None to Report

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

8. CYBER/PRIVACY LOSS HISTORY

If the answer to any question below is "Yes", please provide details for each claim, allegation or incident.

a. In the past 12 months, have you or any other person or organization proposed for this insurance experienced one or more of the following:

- Been served with a lawsuit or received a demand, complaint or charge alleging liability for a privacy breach, privacy injury, security breach, intellectual property infringement or reputational harm;
- Been the subject of any government action, investigation or proceedings regarding any alleged violation of privacy law;
- Notified customers, clients or any third party of any security breach or privacy breach;
- Received any cyber extortion demand or threat;
- Sustained any unscheduled network outage or interruption for any reason (excluding weather conditions and routine service interruptions) that lasted longer than 4 hours;
- Sustained any property damage or business interruption losses as a result of a cyber-attack;
- Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud;
- A business interruption as a direct result of an unscheduled network outage or interruption of a service provider computer system; or
- Became aware of any other cyber security or data privacy event, incident or allegation involving or impacting your organization?

☐ Yes ☐ No

b. Have you notified Tokio Marine HCC of all claims, suits, demands, investigations or inquiries received in the past 12 months?
If "No", forward complete details to Tokio Marine HCC immediately.

☐ Yes ☐ No ☐ None to Report

9. IT DEPARTMENT

This section must be completed by the individual within your organization who is responsible for network security.

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

Name:	Phone:
Title:	Email address:

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 7 through 8 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 & 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 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.

TOKIO MARINE HCC

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