TOKIO MARINE HCC

NetGuard® Plus Cyber Liability Insurance

RANSOMWARE SUPPLEMENTAL APPLICATION

THIS SUPPLEMENTAL APPLICATION IS NOT A BINDER. ***This supplemental application is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this supplemental 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. "You" and "Your", as used in this supplemental application, means the Applicant unless noted otherwise below.***

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 Applicant:

Street Address:

City, State, Zip: Phone:

Website: Fax:

2. IT DEPARTMENT

This section must be completed by the individual within the Applicant's organization who is responsible for network security. As used in this section only, "you" refers only to such individual.

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

Name:

Title:

Phone: Email address:

IT Security Designation(s):

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: _____

d. How many IT personnel are on your team?

e. How many dedicated IT security personnel are on your team?

By signing below, you confirm that you have reviewed all questions in Sections 3 through 5 of this supplemental application regarding the Applicant's security controls, and, to the best of your knowledge, all answers are complete and accurate. Additionally, you consent to 1) the Insurer conducting non-intrusive scans of your internet-facing systems / applications for common vulnerabilities, and 2) receiving direct communications from the Insurer and/or its representatives regarding the results of such scans and any potentially urgent security issues identified in relation to the Applicant's organization.

Print/Type Name: _____

Signature: _____

3. EMAIL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you tag external emails to alert employees that the message originated from outside the organization? ☐ Yes ☐ No

b. Do you pre-screen emails for potentially malicious attachments and links? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Select your email security provider:

If "Other", provide the name of your email security provider: _____

(2) Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user? ☐ Yes ☐ No

c. Have you implemented any of the following to protect against phishing messages? (*check all that apply*):

☐ **Sender Policy Framework (SPF)**
☐ **DomainKeys Identified Mail (DKIM)**
☐ **Domain-based Message Authentication, Reporting & Conformance (DMARC)**
☐ None of the above

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

If "Yes", do you enforce **Multi-Factor Authentication (MFA)**? ☐ Yes ☐ No

e. Do you use Office 365 in your organization? ☐ Yes ☐ No

If "Yes", do you use the Office 365 Advanced Threat Protection add-on? ☐ Yes ☐ No

ADDITIONAL COMMENTS (*Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.*)

4. INTERNAL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you use a cloud provider to store data or host applications? ☐ Yes ☐ No

If "Yes", provide the name of the cloud provider: _____

If you use more than one cloud provider to store data, 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.

b Do you use **MFA** to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? ☐ Yes ☐ No

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

If "Yes", do you use **MFA** to secure all remote access to your network, including any **remote desktop protocol (RDP)** connections? ☐ Yes ☐ No

If **MFA** is used, 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: _____

(3) Does your **MFA** configuration ensure that the compromise of a single device will only compromise a single authenticator? ☐ Yes ☐ No

d. 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: _____

e. 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) Do you enforce application whitelisting/blacklisting? ☐ Yes ☐ No

(3) 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.

(4) Can users access the network with their own device ("Bring Your Own Device")? ☐ Yes ☐ No

If "Yes", is **EDR** required to be installed on these devices? ☐ Yes ☐ No

f. Do you use **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: _____

g. Do you manage privileged accounts using **privileged account management software (PAM)** (e.g., CyberArk, BeyondTrust, etc.)? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Provide the name of your software provider: _____

(2) Is access protected by **MFA**? ☐ Yes ☐ No

h. Do you actively monitor all administrator access for unusual behavior patterns? ☐ Yes ☐ No

If "Yes", provide the name of your monitoring tool: _____

i. Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices? ☐ Yes ☐ No

j. Do you record and track all software and hardware assets deployed across your organization? ☐ Yes ☐ No

If "Yes", provide the name of the tool used for this purpose (if any): _____

k. Do non-IT users have local administration rights on their laptop / desktop? ☐ Yes ☐ No

l. How frequently do you install critical and high severity patches across your enterprise?

☐ 1-3 days ☐ 4-7 days ☐ 8-30 days ☐ One month or longer

m. Do you have any end of life or end of support software? ☐ Yes ☐ No

If "Yes", is it segregated from the rest of your network? ☐ Yes ☐ No

n. Do you use a **protective DNS service (PDNS)** (e.g. ZScaler, Quad9, OpenDNS or the public sector **PDNS** to block access to known malicious websites? ☐ Yes ☐ No

If "Yes", provide the name of your DNS provider: _____

o. Do you use **endpoint application isolation and containment technology** on all endpoints? ☐ Yes ☐ No

If "Yes", select your provider:

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

p. Can users run Microsoft Office Macro enabled documents on their system by default? ☐ Yes ☐ No

q. Do you implement **PowerShell** best practices as outlined in the Environment Recommendations by Microsoft? ☐ Yes ☐ No

r. Do you utilize a **Security Information and Event Management system (SIEM)**? ☐ Yes ☐ No

s. Do you utilize a **Security Operations Center (SOC)**? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Is your **SOC** monitored 24 hours a day, 7 days a week? ☐ Yes ☐ No

(2) Your **SOC** is: ☐ Outsourced; provide the name of your provider: _____

☐ Managed internally/in-house

t. Do you use a **vulnerability management tool**? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Select your provider:

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

(2) What is your patching cadence?

☐ 1-3 days ☐ 4-7 days ☐ 8-30 days ☐ 1 month or longer

ADDITIONAL COMMENTS (*Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.*)

5. BACKUP AND RECOVERY POLICIES

If the answer to the question in this section is "No", please provide additional details in the "Additional Comments" section.

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

If "Yes":

a. Which best describes your data backup solution?

☐ Backups are kept locally but separate from your network **(offline/air-gapped backup solution)**.

☐ Backups are kept in a dedicated cloud backup service.

☐ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

☐ Other (*describe your data backup solution)*: _____

b. Check all that apply:

☐ Your backups are encrypted.

☐ You have **immutable backups**.

☐ Your backups are secured with different access credentials from other administrator credentials.

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

☐ You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months.

☐ You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.

c. How frequently are backups run? ☐ Daily ☐ Weekly ☐ Monthly

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?

☐ 0-24 hours ☐ 1-3 days ☐ 4-6 days ☐ 1 week or longer

ADDITIONAL COMMENTS (*Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.*)

CERTIFICATION, CONSENT AND SIGNATURE

I understand that the information submitted in this supplemental application becomes a part of my Cyber Liability Insurance Application and is subject to the same representations and conditions.

By signing below, the Applicant consents to the Insurer conducting non-intrusive scans of the Applicant's internet-facing systems / applications for common vulnerabilities.

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

The following Cyber Glossary is provided to assist you in completing your application correctly and completely.

DomainKeys Identified Mail (DKIM) is an email authentication method that allows senders to associate a domain name with an email message, thus vouching for its authenticity. A sender creates the DKIM by "signing" the email with a digital signature. This "signature" is located in the message's header.

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication protocol that uses Sender Policy Framework (SPF) and DKIM to determine the authenticity of an email message.

Endpoint application isolation and containment technology is a form of zero-trust endpoint security. Instead of detecting or reacting to threats, it enforces controls that block and restrain harmful actions to prevent compromise. Application containment is used to block harmful file and memory actions to other apps and the endpoint. Application isolation is used to prevent other endpoint processes from altering or stealing from an isolated app or resources.

Common Providers: Authentic8 Silo; BitDefender™ Browser Isolation; CylancePROTECT; Menlo Security Isolation Platform; Symantec Web Security Service

Endpoint Detection and Response (EDR), also known as endpoint *threat* detection and response, 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, unchangeable, and can be deployed to production servers immediately in case of ransomware attacks or other data loss.

Multi-Factor Authentication (MFA) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print). MFA for remote email access can be enabled through most email providers.

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

Next-Generation Anti-Virus (NGAV) is software that uses predictive analytics driven by machine learning and artificial intelligence and combines 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. For purposes of completing this application, NGAV refers to anti-virus protection that focuses on detecting and preventing malware on each individual endpoint. If your organization has a NGAV solution **AND** you are centrally monitoring and analyzing all endpoint activity, please indicate that you have NGAV & EDR on the application.

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

Offline/Air-gapped backup solution refers to a backup and recovery solution in which one copy of your organization's data is 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.

Cyber Glossary

Powershell is a cross-platform task automation and configuration management framework from Microsoft, consisting of a command-line shell and scripting language. It is used by IT departments to run tasks on multiple computers in an efficient manner. For example, Powershell can be used to install a new application across your organization.

Privileged Account Management Software (PAM) is software that allows you to secure your privileged credentials in a centralized, secure vault (i.e., a password safe). To qualify as PAM, a product must allow administrators to create privileged access accounts; offer a secure vault to store privileged credentials; and monitor and log user actions while using privileged accounts.

Common Providers: CyberArk and BeyondTrust.

Protective DNS Service (PDNS) refers to a service that provides Domain Name Service (DNS) protection (also known as DNS filtering) by blacklisting dangerous sites and filtering out unwanted content. It can also help to detect & prevent malware that uses DNS tunneling to communicate with a command and control server.

Common Providers: Zscaler; Quad9; OpenDNS; and public sector PDNS.

Remote Desktop Protocol (RDP) connections is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Security Information and Event Management system (SIEM) is a subsection within the field of computer security, wherein software products and services combine security information management and security event management. SIEM provides real-time analysis of security alerts generated by applications and network hardware.

Security Operations Center (SOC) is a centralized unit that deals with security issues on an organizational and technical level.

Sender Policy Framework (SPF) is an email authentication technique used to prevent spammers from sending messages on behalf of your domain. With SPF, your organization can publish authorized mail servers.

Vulnerability management tool is a cloud service that gives you instantaneous, global visibility into where your IT systems might be vulnerable to the latest internet threats and how to protect against them. The tool is an ongoing process that includes proactive asset discovery, continuous monitoring, mitigation, remediation and defense tactics to protect your organization's modern IT attack surface from cyber threats.

Common Providers: Qualys; InsightVM by Rapid7; and Nessus® by Tenable™

TOKIO MARINE HCC