THIS IS A PROPOSAL FOR A CLAIMS MADE AND REPORTED POLICY. THIS PROPOSAL IS NOT A COVER NOTE.

This proposal for CyberGuard™ Plus Cyber Liability Insurance is intended to be used for the preliminary evaluation of a submission. When signed, this proposal will enable the Underwriter to decide whether or not to authorise the binding of insurance and determine the terms of such 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/proposals. "You" and "Your", as used in this proposal, 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 Primary Applicant:

Business Address: Phone:

Description of operations:

Number of Employees:

2. ADDITIONAL ENTITIES

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

3. WEBSITES / DOMAINS

List all websites and domains owned by you, or operated by/for you, including any other entities for which coverage is sought under the policy:

4. CONFIRMATION OF ENTITIES

This proposal is reflective of the total exposure for all entities seeking coverage, including revenues, records, controls, vendors and loss history. ☐ Yes ☐ No

5. TOTAL GROSS REVENUES

a. Current Full Financial Year:	$
b. Last Completed Full Financial 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 (e.g., name, email, address):

Personally Identifiable Information (PII):

Private health information:

Payment Card Information:

Total unique records:

b. 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 UK, EU, local and foreign laws? ☐ Yes ☐ No

7. DIGITAL MARKETING & CONTENT MANAGEMENT

a. Do you currently use, or have you previously used, any code, software, tool or other technology that tracks, collects or otherwise records website visitor activity, including, but not limited to, Flash Cookies, TikTok Web Beacon, Google Analytics, Meta Pixel, Microsoft Clarity or any similar tracking tool or technology? ☐ Yes ☐ No

If "Yes", select all tracking technologies in use or that will be used:

- ☐ Flash Cookies
- ☐ TikTok Web Beacon
- ☐ Google Analytics
- ☐ Meta Pixel
- ☐ Microsoft Clarity
- ☐ Other: _____

b. Do you use materials provided by others (such as content, video, music, graphics, etc.) on your website, in digital or physical marketing, or for any other business purpose? ☐ Yes ☐ No

If "Yes", do you always obtain the necessary rights, licenses, releases, and consents for the use of these materials? ☐ Yes ☐ No

8. INTERNAL SECURITY CONTROLS

***Note:** By selecting "Yes" to the **Multi-Factor Authentication (MFA)** question, you represent that **MFA** is implemented and enforced prior to the inception of the proposed policy and will remain continuously implemented and enforced for the duration of the policy period.*

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

If "Yes", are all **SSL VPN (Web VPN)** login pages tied to the domain(s) listed in question 3 of this application? ☐ Yes ☐ No

(2) Is **MFA** implemented and 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)** and any **RMM (Remote Management and Monitoring)** applications? ☐ Yes ☐ No

(3) If **MFA** is enforced, complete the following:

Select your **MFA** provider:

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

b. Do you use an **endpoint detection and response (EDR)** tool that provides centralised monitoring and logging and is configured to automatically contain threats for 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 and monitored on 100% of workstations and servers? ☐ 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.

c. Is **MFA** implemented and enforced to secure:

(1) All local access to privileged user accounts? ☐ Yes ☐ No

(2) All remote access to privileged user accounts? ☐ Yes ☐ No

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

If "Yes", is **MFA** implemented and enforced? ☐ Yes ☐ No

e. Do you enforce Account Lockout policies for all users? This includes all users and administrators and other privileged user accounts for all email, firewall, **VPN** and applications that may provide remote access to your network. ☐ Yes ☐ No

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

9. BACKUP AND RECOVERY POLICIES

***Note:** By selecting "Yes" to the **Multi-Factor Authentication (MFA)** question, you represent that **MFA** is implemented and enforced prior to the inception of the proposed policy and will remain continuously implemented and enforced for the duration of the policy period.*

Do you backup all critical applications, servers and data? ☐ Yes ☐ No

If "Yes":

a. Check all that apply:

- ☐ Your backups are **immutable**.
- ☐ Your backups are kept separate from your network **(offline/air-gapped backup solution** or **cloud-based backup solution)**.
- ☐ **MFA** is implemented and enforced to access all backup data.

b. How frequently do you run backups?

c. 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 organisation send and/or receive wire transfers? ☐ Yes ☐ No

If "Yes", does your wire transfer authorisation process include the following:

(1) A wire request documentation form, a protocol for obtaining proper written authorisation 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 that provide services, including IT Services such as SaaS or Cloud or web services. Please provide their services and websites/domains.

Name	Services	Websites/Domains

12. LOSS HISTORY

If the answer to any question in 12.a. through 12.c. below is "Yes", please provide details for each claim, allegation or incident.

a. In the past 3 years, have you or any other individual or entity proposed for this insurance:

(1) Received any complaints, witness summons or other written demands for any relief or been a party to any litigation involving breach of data protection laws (including unauthorised access to, or disclosure of private information), breach of confidence, misuse 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) Received any requests or demands from a third party seeking defence or indemnification? ☐ Yes ☐ No

(3) Received a request for restitution, disgorgement of fees, or termination of contract? ☐ Yes ☐ No

(4) Been the subject of any government action, investigation or other proceedings regarding any alleged breach of data protection or privacy laws (including the UK GDPR or Data Protection Act 2018)? ☐ Yes ☐ No

(5) Notified customers, clients or any third party of any security breach or privacy breach? ☐ Yes ☐ No

(6) Received any cyber extortion demand or threat? ☐ Yes ☐ No

(7) 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

(8) Sustained any property damage or business interruption losses as a result of a cyber-attack or system failure? ☐ Yes ☐ No

(9) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? ☐ Yes ☐ No

b. In the past 3 years, has any service provider with access to your network or computer system(s) sustained an unscheduled network outage or interruption that lasted longer than 4 hours? ☐ Yes ☐ No

If "Yes", did you experience an interruption in business as a result of such outage or interruption? ☐ Yes ☐ No

c. Do you or any other person or organisation 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

13. IT DEPARTMENT

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

a. Within the Applicant's organisation, 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 utilising that are not listed above.

NOTICE TO APPLICANT

The insurance for which you are applying will not respond to claims or incidents about which any person proposed for the insurance had knowledge prior to the effective date of the policy, nor will the insurance coverage apply to any claim, incident or circumstance identified or that should have been identified in questions 12.a. through 12.c of this proposal.

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 proposal 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 proposal does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this proposal is complete and correct, and that all particulars which may have a bearing upon acceptability as a CyberGuard™ Plus Cyber Liability 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 proposal 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 proposal and the requested date for coverage to be incepted, the Applicant becomes aware of any information which would change the answers furnished in response to any question of this proposal, such information shall be revealed immediately in writing to the Underwriter.

This proposal shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by a director or other duly authorised senior representative of the company.

Print or Type Applicant's Name	Title of Applicant
Signature of Applicant	Date Signed by Applicant

CyberGuard™ and CyberNET™ are pending trademark applications in the United Kingdom and Ireland.

Cyber Glossary

TO ASSIST YOU IN COMPLETING YOUR APPLICATION

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

Cloud-Based Backup Solution is a service that stores copies of your data on remote third-party servers.

Endpoint Detection and Response (EDR) centrally collect and analyses comprehensive endpoint data across your entire organisation 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 behaviour, 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 or National Insurance numbers, driver's licence numbers, addresses, passwords, and any other non-public information as defined in the policy form.

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

Tokio Marine HCC is a trading name of HCC International Insurance Company plc, which is a member of the Tokio Marine HCC Group of Companies. HCC International Insurance Company plc is authorised by the Prudential Regulation Authority (PRA) and regulated by the UK Financial Conduct Authority (FCA) and Prudential Regulation Authority. Registered in England and Wales No. 01575839 with registered office at The St Botolph Building, 138 Houndsditch, London, EC3A 7BT, United Kingdom.