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. 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:

Number of Employees:

Website (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):

Attach a list 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.

2. TOTAL GROSS REVENUES

Current Full Financial Year:	£

3. 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):

4. 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", 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

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: _____

5. LOSS HISTORY

In the past 3 years, have you or any other individual or entity proposed for this insurance experienced one or more of the following:

- 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;
- Received any requests or demands from a third party seeking defense or indemnification;
- Received a request for restitution, disgorgement of fees, or termination of contract;
- 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;

☐ Yes ☐ No

- 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 or system failure;
- 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 organisation?

If "Yes", please explain each claim, allegation or incident in detail on a separate sheet.

6. IT DEPARTMENT

This section must be completed by the individual within the Applicant's organisation who is responsible for network security.

Within the Applicant's organisation, 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 claims or incidents about which any person proposed for the insurance had knowledge prior to the inception date of the policy nor will the insurance apply to any claim, incident or circumstance identified or that should have been identified in question 5 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 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

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