PROPOSAL FORM

Important Notice

The applicant should disclose all the facts you know. Any nondisclosed shall make the policy issued hereunder voidable. The company has the right to void the contract and refuse the claims according to the Civil Commercial Code Section 865.

Section I. Proposer Details

1. Company name	
2. Principal address, including postal code	

Section II. Digital Footprint

Please provide the following information which are attributed to the Company.

The Insurer may, but is under no obligation to, (1) use externally observable data about the Company's computer network, and (2) contact the Company's Chief Information Security Officer (or other person designated by the Company) in connection with a condition or circumstance that the Insurer reasonably believes may result in a future event for which coverage may be afforded under the policy being applied for. The Insurer may continue to observe and report, as described above, during the term of any policy containing coverage issued to the Company.

3. Enter Company primary web domain and other web domains the Company has	
4. Enter public (external) IP addresses of the Company including those leased from an Internet Service Provider	
5. Chief Information Security Officer (CISO) or equivalent employee that is responsible for maintaining the Company's cybersecurity posture	Name
	Title
	Email address
6. Date the Company was established	D D M M Y Y Y Y

7. Is the Company a subsidiary of another company? ☐ Yes ☐ No

If yes, please provide the following information:

Name of parent

Registered address

Website

8. Business description

9. Revenue

Currency:

	Prior Year	Current Year (Estimate)
Total Gross Revenue		

Geographical Split of Revenue (%)

Thailand		
Europe		
UK		
United States		
Australia/New Zealand		
Rest of World		

10. Data and System Configuration

(a) Please state the number of data records currently processed/stored by the Company or by a third party in the following categories:

	Thailand		UK/Europe		US/Canada		Rest of world	
	Processed	Stored	Processed	Stored	Processed	Stored	Processed	Stored
PII (Personally Identifiable Information including employee information)								
PHI (Protected Healthcare Information)								
Biometric Identifiers								
PCI (Payment Card Information)								

(b) Are all PCI transactions processed via validated PCI Point-to-Point Encryption (P2PE) Solution**? ☐ Yes ☐ No

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

(c) Does the Company utilise Microsoft Active Directory Domain Services (ADDS), whether "on prem" or hosted, or in a hybrid configuration? This does NOT include Microsoft Entra ID (formerly known as Azure Active Directory or "Azure AD"). ☐ Yes ☐ No

(d) Does the Company utilise Microsoft Exchange, including in a "hybrid deployment"? ☐ Yes ☐ No

(e) Does the Company utilise any unsupported software (software the vendor is no longer providing security fixes for)? ☐ Yes ☐ No

11. Controls

(a) To prevent account takeover (attackers gaining unauthorised access to accounts), does the Company:

(i) require Multi-Factor Authentication (MFA) for all externally exposed applications? Note this includes web-based email such as Microsoft 365 and would mean disabling legacy authentication in addition to enabling MFA. ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) require MFA for remote network access (e.g. for the Virtual Private ☐ Yes ☐ No

Network/VPN)? Please provide comments, if applicable.

(iii) require MFA for administrative access? ☐ Yes ☐ No

Please provide comments, if applicable.

(iv) have a policy against password reuse (use unique passwords for all Company assets)? ☐ Yes ☐ No

Please provide comments, if applicable.

(v) restrict administrator privileges to dedicated accounts (and use separate accounts for general computing)? ☐ Yes ☐ No

Please provide comments, if applicable.

(b) To reduce the effectiveness of phishing attacks against employees, does the Company:

(i) have a Security Awareness Training program that is updated at least annually, and educates the Company's workforce on security best practices? ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) undertake annual phishing simulation exercises for employees or otherwise train them on how to recognise social engineering attacks? ☐ Yes ☐ No

Please provide comments, if applicable.

(iii) "tag" emails from outside the Company (by prepending "External" to the subject line, or similar)? ☐ Yes ☐ No

Please provide comments, if applicable.

(c) To avoid drawing the attention of opportunistic attackers (including continuously scanning for misconfigurations), does the Company:

(i) have a documented secure configuration process for Company assets that is reviewed at least annually? ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) have a documented process to manage vulnerabilities on Company assets that is reviewed at least annually? ☐ Yes ☐ No

Please provide comments, if applicable.

(iii) use an External Attack Surface Monitoring (EASM) service or Cybersecurity Ratings Platform to monitor its internet attack surface and understand how attackers see it? ☐ Yes ☐ No

Please provide comments, if applicable.

(d) To guard against malicious attachments and links, does the Company:

(i) use a Domain Name System (DNS) filtering service to block access to known malicious domains? ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) utilise network-based URL filters such as category-based filtering, reputation-based filtering, or block lists to prevent Company assets from connecting to potentially malicious or unapproved websites? ☐ Yes ☐ No

Please provide comments, if applicable.

(iii) block unnecessary file types (those without a business need) at the email gateway? ☐ Yes ☐ No

Please provide comments, if applicable.

(iv) utilise email server anti-malware protections such as attachment scanning and/or sandboxing to block known malicious or suspicious attachments? ☐ Yes ☐ No

Please provide comments, if applicable.

(e) To protect against malicious software and other threats, does the Company:

(i) deploy and keep updated endpoint security software on all Company assets? ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) utilise an endpoint security software with behavioral-detection and exploit mitigation capabilities? ☐ Yes ☐ No

Please provide comments, if applicable.

(iii) utilise endpoint security software with technical controls to only allow authorised software (e.g. “Application Allowlisting”)? ☐ Yes ☐ No

Please provide comments, if applicable.

(f) To reduce the impact of a lost or stolen device or storage media, does the Company:

(i) maintain a detailed asset inventory with bi-annual or more frequent updates? ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) encrypt data on end-user devices (e.g. Windows BitLocker, Apple FileVault or Linux dm-crypt)? ☐ Yes ☐ No

Please provide comments, if applicable.

(iii) encrypt all data on removeable media? ☐ Yes ☐ No

Please provide comments, if applicable.

(g) To mitigate the impact of an incident, does the Company:

(i) have a documented data recovery process that is updated at least annually (including what data needs to be backed up, its recovery prioritisation, and how such data is secured)? ☐ Yes ☐ No

Please provide comments, if applicable.

(ii) perform automated backups at least weekly? ☐ Yes ☐ No

Please provide comments, if applicable.

(iii) have a documented process for reporting incidents (including who to report to, the mechanism for reporting, the required timeframe and the minimum information to include)? ☐ Yes ☐ No

Please provide comments, if applicable.

12. Insurance History

Please provide details of previous Cyber insurance carried during the past three (3) years:

Policy Period	Insurer	Limit	Excess	Premium

13. Incident and Claims History

During the last five (5) years, have you suffered from any of the following?

(a) the unauthorised disclosure or transmission of any confidential information for which you are responsible	☐ Yes	☐ No
(b) any intrusion of, unauthorised access to, or unauthorised use of your computer system	☐ Yes	☐ No
(c) any accidental, negligence or unintentional act or failure to act by and employee or an employee of any third-party service provider whilst operating, maintaining or upgrading your computer system	☐ Yes	☐ No
(d) the suspension or degradation of your computer system	☐ Yes	☐ No
(e) your inability to access data due to such data being deleted, damaged, corrupted, altered or lost	☐ Yes	☐ No
(f) receipt of an extortion demand or security threat	☐ Yes	☐ No
(g) receipt of a claim in respect of any of the above	☐ Yes	☐ No
(h) any formal or official action, investigation, inquiry or audit by a regulator arising out of your use, control, collection, storing, processing or suspected misuse of personal information	☐ Yes	☐ No

If **yes** to any of the above, please provide details: