

# Allianz Protect<sup>®</sup>

**CYBER PROTECT**

**INSURANCE PROPOSAL FORM**

**Allianz General Insurance Company  
(Malaysia) Berhad** 200601015674 (753426-V)

**IMPORTANT**

Allianz General Insurance Company (Malaysia) Berhad is licensed under the Financial Services Act 2013 (FSA) and regulated by Bank Negara Malaysia (BNM).

**Non-Consumer Insurance Contract**

Pursuant to Paragraph 4 of Schedule 9 of the Financial Services Act 2013, if you are applying for this Insurance **for purposes related to your trade, business or profession**, you have a duty to disclose any matter that you know to be relevant to our decision in accepting the risks and determining the rates and terms to be applied and any matter a reasonable person in the circumstances could be expected to know to be relevant, otherwise it may result in avoidance of contract, claim denied or reduced, terms changed or varied, or contract terminated.

**This duty of disclosure shall continue until the time the contract is entered into, varied or renewed.**

The completion and signature of this proposal form does not bind the Proposer(s) or the Insurer(s) to complete a contract of insurance. If there is insufficient space to answer questions, please use an additional sheet and attach it to this form (please indicate question number).

This is a Proposal Form for a Policy relating to claims made against the Insured during the Policy Period.

**1. GENERAL INFORMATION**

- (a) Name of Policyholder : \_\_\_\_
- (b) Address of Principal Office : \_\_\_\_
- (c) Country of incorporation of the Policyholder : \_\_\_\_
- (e) Date of establishment. : \_\_\_\_
- (f) Website address : \_\_\_\_

**2. BUSINESS INFORMATION**

- (a) Please provide a clear description of the business activities

\_\_\_\_\_

- (b) Please provide the following information for your Company

	<b>Malaysia</b>	<b>USA</b>	<b>EU</b>	<b>ROW</b>
<b>Employee Numbers</b>				
<b>Turnover</b>				
<b>Turnover from Web based trading</b>				
<b>Estimate of customer numbers</b>				
<b>Total Assets</b>				

### 3. INSURANCE PROGRAMME

Please provide the following information

	Limit Requested	Deductible Re- quested	Current Insurer	Current Premium
Standard Cyber Covers				
Business Interruption				

Allianz Cyber Protect includes the following coverage as standard

- Privacy and data breach
- Network security
- Media liability
- Regulatory costs
- Regulatory fines & penalties
- Hacker theft
- Cyber extortion
- Crisis communication
- Consultant services
- E-payment contractual penalties

Some covers may have additional terms and conditions imposed and sub-limits applied.

### 4. POLICIES AND PROCEDURES

(a) Has data security and information technology risk in general been added to your company risk register?

YES       NO

If "**NO**", please provide details: \_\_\_\_

(b) Do you have a written data protection/information security policy?

YES       NO

If "**NO**", please provide details: \_\_\_\_

(c) Does the policy (or in the absence of a policy do you) provide guidance on;

	Yes	No	Comments
Responsibilities of the Information Security Officer or equivalent	<input type="checkbox"/>	<input type="checkbox"/>	
Network security (access rights, passwords, encryption etc)	<input type="checkbox"/>	<input type="checkbox"/>	
Mobile device security (inc. laptops, smart phones and memory devices)	<input type="checkbox"/>	<input type="checkbox"/>	
Use and storage of personally identifiable information & notification in case of a breach.	<input type="checkbox"/>	<input type="checkbox"/>	
Employee's use of social networking websites	<input type="checkbox"/>	<input type="checkbox"/>	
Use of unsecured WiFi networks	<input type="checkbox"/>	<input type="checkbox"/>	
Data backup procedures (please comment on how often backup takes place and whether this is offsite)	<input type="checkbox"/>	<input type="checkbox"/>	

(d) Are all employees trained and/or made aware of the requirements of the policy?

YES       NO

If "NO", please provide details: \_\_\_\_

(e) Are the security standards set by the policy tested, has this involved a qualified security assessor?

YES       NO

Please briefly describe: \_\_\_\_

(f) Is the policy reviewed and updated on a regular basis?

YES       NO

If so how frequently? \_\_\_\_

(g) Do you maintain up to date (generally accepted) data security techniques?

YES       NO

If you comply with any industry standards e.g. ISO 27001, please briefly describe:

\_\_\_\_

## 5. PAYMENT CARD INFORMATION

(a) Do you collect credit/debit or any other type of payment information?

YES       NO

(b) Do you process payments on behalf of any other individual or organisation?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(c) Are you fully compliant with the applicable Payment Card Industry Data Security Standards (PCI DSS)?

YES       NO

Is compliance self certified?

YES       NO

If no, who carries out certification \_\_\_\_\_

## 6. THIRD PARTY SERVICE PROVIDERS

(a) Do you use any third-party service providers to remotely host any activities (e.g web site maintenance, data backup, payment services etc)?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(b) Describe the due diligence carried out by or on your behalf to ensure the service provider's security arrangements are adequate.

\_\_\_\_\_

(c) Does the contract ensure that the third party service provider has a contractual liability for any losses suffered by you for the failure of the service provide to adequately protect the insured's data?

YES       NO

If "YES", please provide details: \_\_\_\_\_

Is this liability limited, if so at what level? \_\_\_\_\_

## 7. CRISIS MANAGEMENT

(a) Do you have a written crisis management plan that address breaches of data and network security?

YES       NO

(b) How often is this reviewed and updated? \_\_\_\_\_

(c) Have you identified third party service providers to help you with crisis management and response?

YES       NO

If "YES", please provide details: \_\_\_\_\_

## 8. HISTORICAL LOSSES AND INCIDENTS

In the last 5 years;

(a) Have you notified any claims or circumstances under a liability policy (e.g. Cyber liability, general liability, D&O liability, E&O etc) or any other insurance policy (property, B.I etc) arising from a

breach of privacy, loss or theft of personal or commercial information or the unauthorised access of your computer network?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(b) Has a regulator or recognised industry body ever investigated you in respect of personally identifiable information or requested information from you in this regard?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(c) Have you ever received a complaint from a customer, employee or service provider in respect of their personally identifiable (or corporate) information?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(d) Have you been the subject of a targeted attack on your computer system?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(e) Has your computer network/system been suspended or interrupted (voluntarily or otherwise) for any reason (e.g targeted or generalised attack, loss of data etc)?

YES       NO

If "YES", please provide details: \_\_\_\_\_

(f) How long did the suspension or interruption last? \_\_\_\_\_

(g) Was there a loss of profits or an increase of costs associated with the suspension or interruption?

YES       NO

If "YES", please provide details: \_\_\_\_\_

## 9. WARRANTY STATEMENT

(a) Are you aware, after inquiry of any facts or circumstances that may give rise to a claim under the proposed policy?

YES       NO

If "YES", please provide details: \_\_\_\_\_

---

I/We understand and agree that any information provided herein and/or in any other related document may be provided to third parties in relation to the insurance cover applied for including without limitation, vendors, reinsurers and professional advisers. For the avoidance of doubt, such consent applies to all information provided by the undersigned for and/or on behalf of the proposed insured(s), where applicable.

I DECLARE that the above statements are true and complete to the best of my knowledge and belief and that no material facts have been misstated or suppressed after reasonable enquiry. I undertake to inform insurers of any material alteration to those facts occurring before inception of the insurance.

A material fact is one which would influence the acceptance or assessment of the risk.

---

Signed \_\_\_\_\_

Chairman/Chief Executive/Managing Director

(This form must be signed by the Chairman, Chief Executive or Managing Director)

Company \_\_\_\_

Date \_\_\_\_

---

**Applicable Tax**

In the event that any sales and services tax, value added tax or any similar tax and any other duties, taxes, levies or imposts (collectively "**Applicable Tax**") whatsoever are introduced by any authority and are payable under the laws of Malaysia in connection with any supply of goods and/or services made or deemed to be made under this Policy, We will be entitled to charge any Applicable Tax as allowed by the laws of Malaysia. Such Applicable Tax payable shall be paid in addition to the applicable premiums and other charges. All provisions in this Policy on payment of premiums and default hereof shall apply equally to the Applicable Tax.

## Cyber Supplementary Questionnaire (applicable to all entities of the organisation)

Please provide a breakdown of the estimated no of records store, transmitted or processed:

Data Type	RoW	EU	USA
Personally Identifiable Data			
Payment Card Data			
Health Information			
Others (please describe)			
<b>Total</b>			

Please respond to the below questions providing yes / no answers, including additional commentary where appropriate.

Policies and Risk Management	
Data privacy and information security awareness training (including social engineering or phishing issues) are conducted at least annually.	<input type="checkbox"/> YES <input type="checkbox"/> NO
The company's due diligence process covers cybersecurity assessment in place for mergers and acquisitions and the networks kept entirely separated until cybersecurity elevated to a satisfactory level.	<input type="checkbox"/> YES <input type="checkbox"/> NO
There are cybersecurity governance processes in place with clearly defined responsibilities for Technology/Security and covering third-party service providers.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Continuity & Backup	
Cyber Incident response plans covering business continuity, disaster recovery elements defined and tested at least annually.	<input type="checkbox"/> YES <input type="checkbox"/> NO
There is a documented backup policy in placed and enforced.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Backups are restored and tested for critical systems and data at least annually.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Network Security & Operations	
With respect to the Company's monitoring and detection tools, please indicate all that apply:	
Firewall configuration	<input type="checkbox"/> YES <input type="checkbox"/> NO
Intrusion detection system	<input type="checkbox"/> YES <input type="checkbox"/> NO
Antivirus software	<input type="checkbox"/> YES <input type="checkbox"/> NO
Endpoint protection	<input type="checkbox"/> YES <input type="checkbox"/> NO
Mail content filtering	<input type="checkbox"/> YES <input type="checkbox"/> NO
24 x 7 monitoring for security violations of critical applications	<input type="checkbox"/> YES <input type="checkbox"/> NO
Penetration testing is conducted at least annually to assess the security of its externally facing systems.	<input type="checkbox"/> YES <input type="checkbox"/> NO
There is a defined patch management process to regularly deploy system patches.	<input type="checkbox"/> YES <input type="checkbox"/> NO
There are physical and/or logical segregations maintained within the network including the cloud environment.	<input type="checkbox"/> YES <input type="checkbox"/> NO
If you have any end of life or end of support software, is it segregated from the rest of the network?	<input type="checkbox"/> YES <input type="checkbox"/> NO
Data/Access Controls	
Appropriate access control policies are implemented for all users, with special consideration to the privileged accounts.	<input type="checkbox"/> YES <input type="checkbox"/> NO



Sensitive and confidential information are encrypted while:	
At rest (on your databases and servers)	<input type="checkbox"/> YES <input type="checkbox"/> NO
When in transit from the network	<input type="checkbox"/> YES <input type="checkbox"/> NO
On back-up disks	<input type="checkbox"/> YES <input type="checkbox"/> NO
Access to sensitive information on your network is tracked and monitored.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Advanced authentication controls like two-factor and certificates are in place for remote access (by employees and third party vendors).	<input type="checkbox"/> YES <input type="checkbox"/> NO
<b>Disaster Recovery Capabilities</b>	
Does the company test its ability to restore different critical systems and data in a timely fashion from its backups at least annually?	<input type="checkbox"/> YES <input type="checkbox"/> NO
With respect to backup capabilities, please advise if the backup strategy includes:	
offline backups (can be stored on site)	<input type="checkbox"/> YES <input type="checkbox"/> NO
offline backups stored offsite	<input type="checkbox"/> YES <input type="checkbox"/> NO
Please indicate the company's Recovery Time Objective (RTO) for critical systems.	
<4 hrs	<input type="checkbox"/> YES <input type="checkbox"/> NO
<4-24 hours	<input type="checkbox"/> YES <input type="checkbox"/> NO
1-2 days	<input type="checkbox"/> YES <input type="checkbox"/> NO
None defined	
<b>Log4j vulnerability</b>	
Please confirm the company has implemented the following:	
An active campaign started to detect, hunt and prevent CVE-2021-44228 Log4j 2 exploitation.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Intensified scanning, monitoring and incident response efforts to identify and contain the attack at an early stage.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Routinely run vulnerability (yellow – orange – red) scanning across the networks to detect when updates are available.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Firewall rules reviewed and updated frequently in response to the emerging attack patterns as required.	<input type="checkbox"/> YES <input type="checkbox"/> NO
Up-to-date information on threats and vulnerabilities received on a regular and on an active basis, e.g., CERT.	<input type="checkbox"/> YES <input type="checkbox"/> NO
<b>CrowdStrike</b>	
Please confirm the company has implemented the following:	
Has your company been impacted by the recent outage caused by CrowdStrike?	<input type="checkbox"/> YES <input type="checkbox"/> NO

<p>If yes, what is the current position of your company in dealing with the outage such as:</p>	
<p>a) Any measures have been implemented to mitigate the impact from the CrowdStrike/Microsoft outage? E.g., Business Continuity Planning scenario testing to ensure continuity of the most critical business operations.</p>	
<p>b) Is the insured in active discussion with its suppliers, software vendors, MSSP to see if they have remediated the CrowdStrike/Microsoft outage in their environment?</p>	
<p>c) Others (Please provide details).</p>	