Chubb Cyber Enterprise Risk Management Insurance

Proposal Form

Instructions to the Applicant

A. This proposal **must be completed, signed and dated by a Principal, Partner or Director**.

B. You must answer **all** the questions in this form. If a question is not applicable, state **"N/A"**. If more space is required to answer a question, continue on your letterhead.

C. If you are a new business, use the projected figures from your business plan.

D. If you have any questions concerning this proposal, please contact your insurance broker or adviser to discuss.

Application for Insurance Cover

Period of Insurance	**From**	**To**
Limit of Insurance Required	Option 1 RM	Option 2 RM
Excess/Deductible Requested	Option 1 RM	Option 2 RM

1. Details of Applicant

1.1	Names and Company Registration Numbers of all firms applying to be covered under this insurance (Referred to as "You" in the rest of this form)	
1.2	What is your address?	
1.3	What is your website address?	
1.4	When was your firm established?	(day) (month) (year)
1.5	What is the number of your employees?	

1.6 What is your total turnover or fee income for the

	Year	**Malaysia**	**Foreign**	**Total**
Coming year (est)		RM	RM	RM
Current Year (est)		RM	RM	RM
Past year		RM	RM	RM

1.7 Please state your annual gross margin

1.8 What percentage of your fee income is derived from work in

Malaysia	**Other Asia**	**Australia/NZ**	**Europe**	**USA/Canada**	**Others**	**Total**
%	%	%	%	%	%	100 %

2. Details of Business

2.1 Please describe the main business operations of the company/companies to be insured. If these activities include e-commerce, please indicate the percentage of turnover generated

2.2 Please list the companies and subsidiaries to be insured. If the company has subsidiaries outside of Malaysia, please provide the details.

2.3	**Criticality of the Information Systems** Please assess the outage period over which your company will suffer significant impact to its business.

Application (or Activity)	Maximum outage period before adverse impact on business				
	Immediate	> 12 h	> 24 h	> 48 h	> 5 days

3. Information Systems

3.1		< 100	101 - 1000	> 1000
	Number of Information Systems users			
	Number of Laptops			
	Number of Servers			

3.2	Do you have an e-commerce or an online service website?	☐ Yes	☐ No
	If **Yes**: What is the revenue share generated or supported by the website? (estimate)		(% or ME)

4. Information Security (IS)

4.1	Security Policy and Risk Management		
4.1.1	An IS policy is formalised and approved by company management and/or security rules are defined and communicated to all staff and approved by the staff representatives.	☐ Yes	☐ No
4.1.2	Formalised awareness training on the IS is required of all staff at least annually.	☐ Yes	☐ No
4.1.3	You identify critical information systems risks and implement appropriate controls to mitigate them.	☐ Yes	☐ No
4.1.4	Regular audits of the IS are conducted and resulting recommendations are prioritised and implemented	☐ Yes	☐ No
4.1.5	Information resources are inventoried and classifed according to their criticality and sensitivity.	☐ Yes	☐ No
4.1.6	Security requirements that apply to information resources are defined according to classification.	☐ Yes	☐ No

4.2	**Information Systems Protection**		
4.2.1	Access to critical information systems requires dual authentication	☐ Yes	☐ No
4.2.2	Users are required to regularly update passwords	☐ Yes	☐ No
4.2.3	Access authorisations are based on user roles and a procedure for authorisation management is implemented	☐ Yes	☐ No
4.2.4	Secured configurations references are defined for workstations, laptops, servers and mobile devices	☐ Yes	☐ No
4.2.5	Centralised management and configuration monitoring of computer systems are in place	☐ Yes	☐ No
4.2.6	Laptops are protected by a personal firewall	☐ Yes	☐ No
4.2.7	Antivirus software is installed on all systems and antivirus updates are monitored	☐ Yes	☐ No
4.2.8	Security patches are regularly deployed	☐ Yes	☐ No
4.2.9	A Disaster Recovery Plan is implemented and updated regularly	☐ Yes	☐ No
4.2.10	Data backups are performed daily, backups are tested regularly and a backup copies are placed regularly in a remote location	☐ Yes	☐ No
4.3	**Network Security and Operations**		
4.3.1	Traffic filtering between the internal network and internet is updated and monitored regularly	☐ Yes	☐ No
4.3.2	Intrusion detection/prevention system is implemented, updated and monitored regularly	☐ Yes	☐ No
4.3.3	Internal users have access to Internet web site browsing through a network device (proxy) equipped with antivirus and website filtering	☐ Yes	☐ No
4.3.4	Network segmentation is implemented to separate critical areas from non critical areas	☐ Yes	☐ No
4.3.5	Penetration testing is conducted regularly and a remediation plan is implemented where necessary	☐ Yes	☐ No
4.3.6	Vulnerability assessments are conducted regularly and a remediation plan is implemented where necessary	☐ Yes	☐ No
4.3.7	Procedures for incident management and change management are implemented	☐ Yes	☐ No
4.3.8	Security events such as virus detection, access attempts, etc..., are logged and monitored regularly	☐ Yes	☐ No
4.4	**Physical Security of Computing Room**		
4.4.1	Critical systems are placed in at least one dedicated computer room with restricted access and operational alarms are routed to a monitoring location	☐ Yes	☐ No
4.4.2	The data centre hosting critical systems has resilient infrastructure including redundancy of power supply, air conditioning, and network connections	☐ Yes	☐ No
4.4.3	Critical systems are duplicated according to Active/Passive or Active/Active architecture	☐ Yes	☐ No
4.4.4	Critical systems are duplicated on two separate premises	☐ Yes	☐ No

4.4.5	Fire detection and automatic fire extinguishing system in critical areas are implemented	☐ Yes	☐ No
4.4.6	The power supply is protected by a UPS and batteries which are both maintained regularly	☐ Yes	☐ No
4.4.7	Power is backed up by an electric generator which is maintained and tested regularly	☐ Yes	☐ No

4.5 Outsourcing

Please fill in if a function of the information system is out sourced.

4.5.1	The outsourcing contract includes security requirements that should be observed by the service provider	☐ Yes	☐ No
4.5.2	Service Level Agreements (SLA) are defined with the outsourcer to allow incident and change control and penalties are applied to the service provider in case of non compliance with the SLA	☐ Yes	☐ No
4.5.3	Monitoring and steering committee(s) are organised with the service provider for the management and the improvement of the service	☐ Yes	☐ No
4.5.4	You have not waived your rights of recourse against the service provider in the outsourcing contract	☐ Yes	☐ No

What are the outsourced Information Systems functions?			Please specify the Service Provider (Outsourcer)
Desktop management	☐ Yes	☐ No	
Server management	☐ Yes	☐ No	
Network management	☐ Yes	☐ No	
Network security management	☐ Yes	☐ No	
Application management	☐ Yes	☐ No	
Use of cloud computing If **Yes**, please specify the nature of cloud services:	☐ Yes	☐ No	
Software as a Service	☐ Yes	☐ No	
Platform as a Service	☐ Yes	☐ No	
Infrastructure as a Service	☐ Yes	☐ No	
Others, please specify			

4.5.5	The outsourcing contract contains a provision requiring the service provider(s) to maintain professional indemnity or errors and omissions insurance	☐ Yes	☐ No

5. Personal Data Held by the Organisation

5.1	**Type and Number of records**					
5.1.1	The Number of personal information records held for the activity to be insured:					
	Per region					
	Malaysia	**Other Asia**	**Australia/NZ**	**Europe**	**USA/Canada**	**Others**
5.1.2	**Categories of personal data collected/processed**				**Number of records**	
	Commercial and marketing information	☐ Yes	☐ No			
	Payment Card or financial transactions information	☐ Yes	☐ No			
	Health information	☐ Yes	☐ No			
	Others, please specify					
5.1.3	Do you process data for:	☐ your own purpose?		☐ On behalf of third party		
5.2	**Personal Information Protection Policy**					
5.2.1	A privacy policy is formalised and approved by management and/or personal data security rules are defined and communicated to the concerned staff				☐ Yes	☐ No
5.2.2	Awareness and training are provided at least annually to the personnel authorised to acces or process personal data				☐ Yes	☐ No
5.2.3	A personal data protection officer is designated in your organisation				☐ Yes	☐ No
5.2.4	A confidentiality agreement or a confidentiality clause in the employment contract is signed by the concerned staff				☐ Yes	☐ No
5.2.5	The legal aspects of the privacy policy are validated by a lawyer/legal department				☐ Yes	☐ No
5.2.6	Monitoring is implemented to ensure compliance with laws and regulations for the protection of personal data				☐ Yes	☐ No
5.2.7	Your personal information practices have been audited by an external auditor within the past two years				☐ Yes	☐ No
5.2.8	A Data Breach Response plan is implemented and roles are clearly communicated to the functional team members				☐ Yes	☐ No
5.3	**Collection of Personal Data**					
5.3.1	You have notified to the Personal Data Protection Commission (PDPC) the personal data processing involved by your company and you have obtained the applicable PDPC authorisation				☐ Yes	☐ No
5.3.2	A privacy policy is posted on your website which has been reviewed by a lawyer/legal department				☐ Yes	☐ No
5.3.3	Consent of individuals is required before collecting their personal data and the concerned persons can access and if necessary correct or delete their personal data				☐ Yes	☐ No

5.3.4	Recipients are provided with a clear means to opt out of targeted marketing operations	☐ Yes	☐ No
5.3.5	You transfer Personal Data to third parties	☐ Yes	☐ No
	If **Yes**, please answer the following:	☐ Yes	☐ No
	(a) The third party (e.g processor) has a contractual obligation to process personal data only on your behalf and under your instructions	☐ Yes	☐ No
	(b) The third party has a contractual obligation to set up sufficient security measures to protect personal data	☐ Yes	☐ No
5.4	**Personal Information Protection Controls**		
5.4.1	Access to personal data is restricted to only those users who need it to perform their task and access authorisations are reviewed regularly	☐ Yes	☐ No
5.4.2	Personal data is encrypted when stored on information systems and personal data backups are encrypted	☐ Yes	☐ No
5.4.3	Personal data is encrypted when transmitted over the network	☐ Yes	☐ No
5.4.4	Mobile devices and laptop hard disks are encrypted	☐ Yes	☐ No
5.4.5	IS policy prohibits the copying of non encrypted personal data to removable storage devices or transmitting such data via emailtransmission	☐ Yes	☐ No
5.4.6	If personal records held contain payment card information (PCI), please answer the following: Your PCI DSS level is:		
	Level 1 : / Level 2 : / Level 3 : / Level 4:		
5.4.7	The payment processor (yourself or third party) is PCI DSS compliant	☐ Yes	☐ No
	If **No**:		
	PCI is stored encrypted or only a part of payment card numbers is stored	☐ Yes	☐ No
	PCI retention time does not exceed the duration of payment and legal/regulatory requirements	☐ Yes	☐ No
5.4.8	Payment card data processing is externalised	☐ Yes	☐ No
	If **Yes**:		
	You require the payment processor to indemnify you in case of security breach	☐ Yes	☐ No
	Please indicate payment processor name, PCI retention time and any additional security measures:		

5.5	Please provide a description of any information security or privacy incidents that have occurred in the last 36 months. Incidents include any unauthorised access to any computer, computer system, database, intrusion or attacks, denial of use of any computer or system, intentional disruption, corruption, or destruction of data, programs, or applications, any cyber extortion event(s); or any other incidents similar to the foregoing including those that have resulted in a claim, administrative action, or regulatory proceeding.	
	Date	**Description of the incident**

6.0 Insurance History

6.1	Do you currently have similar insurance? If yes, please provide details				☐ Yes	☐ No
	Period of Insurance	**Insurer**	**Policy Limit**	**Excess**	**Retroactive Date**	
			RM	RM		
6.2	Has any application for similar insurance been refused, or has any similar insurance ever been rescinded or cancelled? If yes, please provide details				☐ Yes	☐ No

7.0 Claims Experience

7.1	Have any claims ever been made, or lawsuits been brought against you, your predecessors in business, or any current or former Principals, Partners, Directors, employees, or any other person or entity applying to be insured under this proposed contract of insurance?	☐ Yes	☐ No
7.2	Are any of the Principals, Partners, Directors or employees aware, **after inquiry**, and as of the date of signing this application, of any errors, omissions, offences, circumstances or allegations which might result in a claim being made against you or any person or entity applying to be insured under this proposed contract of insurance?	☐ Yes	☐ No
7.3	Have you, your predecessors in business, or any current or former Principals, Partners, Directors, or employees ever been the subject of disciplinary action or investigation by any authority or regulator or professional body?	☐ Yes	☐ No

If Yes to any of the question in this section, please **provide full details** and the **status** of each claim, lawsuit, allegation or matter, including:

- the date of the claim, suit or allegation
- the date you notified your previous insurers
- the name of the claimant and the project
- the allegations made against you
- the amount claimed by the claimant

- whether the status is outstanding or finalised
- the amounts paid for claims and defence costs to date

Declaration

- We have read and understood the Important Notices contained in this application.
- We agree that this proposal, together with any other information or documents supplied, shall form the basis of any contract of insurance.
- We acknowledge that if this proposal is accepted, the contract of insurance will be subject to the terms and conditions as set out in the policy wording as issued or as otherwise specifically varied in writing by Chubb.
- We declare, **after enquiry,** that the statements, particulars and information contained in this application and in any documents accompanying this application are true and correct in every detail and that no other material facts have been misstated, suppressed or omitted.
- We undertake to inform Chubb of any material alteration to those facts before completion of the contract of insurance.

This form **must** be reviewed, signed and dated by a duly authorised Principal, Partner or Director.

Signed, Principal/Partner/Director:

_____ Date:

Name of signatory

Chubb Cyber Enterprise Risk Management Insurance Proposal Form. Malaysia. Published 05/2016

Important Notices to the Applicant

Your duty of Disclosure :

Before you enter into a contract of general insurance with an Insurer, you have a duty to disclose to the Insurer every matter within your knowledge that is material to the Insurer's decision whether to accept the risk of the insurance and, if so, on what terms.

You have the same duty to disclose those matters to the Insurer before you renew, extend, vary or reinstate a contract of general insurance.

It is important that all information contained in this application is understood by you and is correct, as you will be bound by your answers and by the information provided by you in this application. You should obtain advice before you sign this applicaton if you do not properly understand any part of it

Your duty of disclosure continues after the application has been completed up until the contract of insurance is entered into.

Non-Disclosure:

If you fail to comply with your duty of disclosure, the Insurer may have the option of avoiding the contract of insurance from its beginning.

If your non-disclosure is fraudulent, the Insurer may also have the right to keep the premium that you have paid.

Change of Risk or Circumstances:

You should advise Chubb as soon as practicable of any change to your normal business as disclosed in the application, such as changes in business activities, location, acquisitions and new overseas activities.

Subrogation

Where you have agreed with another person or company (who would otherwise be liable to compensate you for any loss or damage which is covered by the contract of insurance) that you will not seek to recover such loss or damage from that person, Chubb will not cover you, to the extent permitted by law, for such loss or damage.

Privacy Notice / *Notis Privasi*

In line with the Personal Data Protection Act 2010 ("**PDPA**"), we are required to inform you that the personal data you have provided to us or that is subsequently obtained by us from time to time ("**Personal Data**"), may be processed for the purpose of processing your insurance application/proposal, provision of insurance related products or services or any addition, alteration, variation, cancellation, renewal or reinstatement thereof, performing statistical/actuarial research or data study, promoting products and services and other related purposes (collectively, "**Purpose**"). The Personal Data is obtained when you fill up documents; liaise with us or our representatives; or give it to us or our representatives in person, over the telephone, through websites or from third parties you have consented to.

Although you are not obliged to provide us with your Personal Data, we will not be able to process your application for insurance cover or process your claim if you fail to provide all requested information.

Your Personal Data may be disclosed to our related company or any other company carrying on insurance or reinsurance related business, an intermediary, or a claims, investigation or other service provider and to any association, federation or similar organisation of insurance companies that exists or is formed from time to time for the Purpose or to fulfil some legal or regulatory function or is reasonably required in the interest of the insurance industry. In such instances, it will be done in compliance with the PDPA.

We may also disclose your Personal Data where such disclosure is required under the law, court orders or pursuant to guidelines issued by regulatory or other relevant authorities, if we reasonably believe that we have a lawful right to disclose your Personal Data to any third party or that we would have had your consent for such disclosure if you had known of the same, and/or if the disclosure is in the public interest.

Your Personal Data may also be transferred to our related companies and third party providers, which may be located outside Malaysia for the Purpose. In the event that we use external service providers, specific security and confidentiality safeguards have been put in place to ensure your privacy rights remain unaffected.

Where you have given us personal data that is of another individual ("**Data Subject**"), you must ensure that you have informed the Data Subject that you are providing the Data Subject's personal data to us, and have gotten the Data Subject's consent to do so. You must explain what is stated here to the Data Subject, and ensure he/she understands, agrees and authorises us to deal with his/her personal data according to what is stated here.

You may make inquiries, complaints, request for access to or correction of your Personal Data, or limit the processing of your Personal Data at any time hereafter by submitting such request to us at **Chubb Insurance Malaysia Berhad**, Manager, Customer Service Unit, Wisma Chubb, 38 Jalan Sultan Ismail, 50250 Kuala Lumpur, Malaysia (Tel: 03-2058 3000 / E-mail: Inquiries.MY@chubb.com).

By continuing to deal with us, you understand, agree and consent to the terms above with respect to the processing of your Personal Data.

Selaras dengan Akta Perlindungan Data Peribadi 2010 ***("PDPA")****, kami telah diminta untuk memberitahu anda bahawa data peribadi anda berikan kepada kami atau yang selepasnya kami perolehi dari semasa ke semasa ("****Data Peribadi****") mungkin diproses untuk tujuan memproses permohonan/cadangan insurans, penyediaan produk atau perkhidmatan berkaitan insurans atau sebarang penambahan, pindaan, pembatalan, pembaharuan atau penyambungan, pelaksanaan penyelidikan statistik/aktuari atau kajian data, promosi produk dan perkhidmatan dan untuk tujuan lain yang berkaitan (secara bersama, "****Tujuan****"). Data Peribadi tersebut adalah diperolehi apabila anda mengisi dokumen-dokumen; berhubung dengan kami atau wakil-wakil kami; atau memberikan ia kepada kami atau wakil-wakil kami secara peribadi, melalui telefon, atau melalui laman-laman web atau daripada pihak-pihak ketiga yang anda telah bersetuju.*

Walaupun anda tidak diwajibkan untuk memberi kami Data Peribadi anda, kami tidak dapat menimbang permohonan anda untuk perlindungan insurans atau memproses tuntutan anda jika anda tidak memberikan semua maklumat yang diminta.

Data Peribadi anda mungkin akan didedahkan kepada syarikat berkaitan kami atau mana-mana syarikat lain yang menjalankan perniagaan berkaitan insurans atau insurans semula, syarikat perantara, atau sesuatu tuntutan, penyiasatan atau penyedia perkhidmatan lain dan kepada mana-mana persatuan, persekutuan atau organisasi syarikat insurans serupa yang wujud atau yang ditubuhkan dari masa ke masa untuk Tujuan tersebut atau untuk memenuhi fungsi perundangan atau peraturan atau diperlukan dengan sewajarnya demi kepentingan industri insurans. Dalam keadaan sedemikian, ia akan dilakukan mengikuti PDPA.

Kami juga mungkin akan mendedahkan Data Peribadi anda apabila pendedahan sedemikian diperlukan di bawah undang-undang, atas arahan-arahan mahkamah atau menurut garis panduan yang dikeluarkan oleh pihak berkuasa kawal selia atau pihak berkuasa lain, jika kami percaya bahawa kami mempunyai hak di bawah undang-undang untuk mendedahkan Data Peribadi anda kepada mana-mana pihak ketiga atau mungkin akan mendapatkan persetujuan bagi pendedahan tersebut jika anda mengetahui tentangnya, dan/atau jika pendedahan adalah berasaskan kepentingan umum.

Data Peribadi anda juga boleh dipindahkan kepada syarikat-syarikat berkaitan kami dan pembekal-pembekal pihak ketiga yang mungkin terletak di luar Malaysia untuk Tujuan tersebut. Sekiranya kami menggunakan penyedia perkhidmatan luar, langkah-langkah keselamatan dan kerahsiaan tertentu telah pun diambil untuk memastikan hak kerahsiaan anda tidak terjejas.

*Apabila anda memberikan kepada kami data peribadi individu lain ("**Subjek Data**"), anda mestilah memastikan bahawa anda telah memaklumkan kepada Subjek Data bahawa anda akan memberikan data peribadi Subjek Data kepada kami, dan telah mendapati persetujuan Subjek Data untuk berbuat sedemikian. Anda hendaklah menjelaskan apa yang telah dinyatakan di sini kepada Subjek Data, dan memastikannya memahami, bersetuju dan membenarkan anda untuk berurusan dengan data peribadinya mengikuti apa yang dinyatakan di sini.*

*Anda boleh membuat pertanyaan, aduan atau permintaan untuk mendapatkan atau membetulkan Data Peribadi anda atau mengehadkan pemprosesan Data Peribadi pada bila-bila masa selepas ini dengan mengemukakan permintaan tersebut menerusi **Chubb Insurance Malaysia Berhad**, Pengurus, Unit Khidmat Pelanggan, Wisma Chubb, 38 Jalan Sultan Ismail , 50250 Kuala Lumpur, Malaysia (Tel: 03-2058 3000 / E-mail: Inquiries.MY@chubb.com).*

Dengan terus berurusan dengan kami, anda memahami, membenarkan dan bersetuju dengan terma-terma di atas mengenai pemprosesan Data Peribadi anda.

Contact Us

Chubb Insurance Malaysia Berhad
(*formerly known as ACE Jerneh Insurance Berhad*) (9827-A)
(Licensed under the Financial Services Act 2013 and regulated by Bank Negara Malaysia)
Wisma Chubb,
38, Jalan Sultan Ismail,
50200 Kuala Lumpur,
Malaysia
O: +603-2058 3000
F: +603 2058 3333
Inquiries.MY@chubb.com
www.chubb.com/my