# Chubb Cyber Enterprise Risk Management Insurance

## Proposal Form

CHUBB®

## Important Notices

### 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 that you know, or could reasonably be expected to know, is relevant 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.

Your duty however does not require disclosure of any matter:

- that diminishes the risk to be undertaken by the Insurer;
- that is of common knowledge;
- that your Insurer knows or, in the ordinary course of its business, ought to know;
- as to which compliance with your duty is waived by the Insurer.

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

Your duty of disclosure continues after the proposal 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 be entitled to avoid the contract from its beginning.

If your non-disclosure is fraudulent, the Insurer may also have the option of avoiding the contract from its beginning, to retain any premium that you have paid for this contract of insurance.

### Claims Made Contract

Subject to its terms and conditions the policy will cover your legal liability for any claim:

- first made against you during the policy period;
- resulting from any circumstance of which you become aware during the policy period which may give rise to a future claim against you provided you immediately inform us in writing of such circumstances within the policy period.

The Policy will not cover your legal liability resulting from any claim, matter, occurrence or circumstance arising from any act, error or omission committed or alleged to have been committed of which you were aware before commencement of the policy period.

### Change of Risk or Circumstances

You should advise the Insurer as soon as practicable of any change to your normal business as disclosed in the proposal, such as changes in 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 policy, that you will not seek to recover such loss or damage from that person, the Insurer will not cover you, to the extent permitted by law, for such loss or damage.

## 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.

This document allows Chubb to gather the needed information to assess the risks related to the information systems of the prospective insured. Please note that completing this proposal form does not bind Chubb nor the prospective insured to conclude an insurance policy . If the Information Systems Security Policy of the companies/subsidiaries of the prospective insureds vary, please complete the proposal form for each prospective insured.

| **1. Identification of the applicant company** | | | |
|---|---|---|---|
| Company name: | | | |
| Address: | | | |
| | | Post code City: | |
| Website(s): | | | |
| Number of employees: | Annual Turnover: | | Annual Gross Margin: |
| Percentage of turnover generated from: | Asia: | Europe: | Hong Kong: |
| | US/Canada: | Australia: | Rest of the world: |

## 2. Profile of the company/companies to be insured

### 2.1 Business operations

[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 Scope

[The companies and subsidiaries to be insured. If the company has subsidiaries outside of Hong Kong, 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

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

| | Yes | No |
|---|---|---|
| Do you have an e-commerce or an online service website? | ☐ | ☐ |
| If YES:<br>What is the revenue share generated or supported by the website? (estimate) | (%) | |

## 4. Information security (IS)

| 4.1 Security policy and risk management | | Yes | No |
|---|---|---|---|
| 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<br>If yes, please attached the copy of IS policy | ☐ | ☐ |
| 2 | Formalised awareness training on the IS is required of all staff at least annually | ☐ | ☐ |
| 3 | You identify critical information systems risks and implement appropriate controls to mitigate them | ☐ | ☐ |
| 4 | Regular audits of the IS are conducted and resulting recommendations are prioritised and implemented | ☐ | ☐ |

| | | | |
|---|---|---|---|
| 5 | Information resources are inventoried and classified according to their critically and sensitivity | ☐ | ☐ |
| 6 | Security requirements that apply to information resources are defined according to classification | ☐ | ☐ |
| **4.2 Information systems protection** | | **Yes** | **No** |
| 1 | Access to critical information systems requires dual authentication | ☐ | ☐ |
| 2 | Users are required to regularly update passwords | ☐ | ☐ |
| 3 | Access authorisations are based on user roles and a procedure for authorisation management is implemented | ☐ | ☐ |
| 4 | Secured configurations references are defined for workstations, laptops, servers and mobile devices | ☐ | ☐ |
| 5 | Centralised management and configuration monitoring of computer systems are in place | ☐ | ☐ |
| 6 | Laptops are protected by a personal firewall | ☐ | ☐ |
| 7 | Antivirus software is installed on all systems and antivirus updates are monitored | ☐ | ☐ |
| 8 | Security patches are regularly deployed | ☐ | ☐ |
| 9 | A Disaster Recovery Plan is implemented and updated regularly<br>If yes, please attached the copy of Disaster Recovery Plan | ☐ | ☐ |
| 10 | Data backups are performed daily, backups are tested regularly and a backup copies are placed regularly in a remote location | ☐ | ☐ |
| **4.3 Network security and operations** | | **Yes** | **No** |
| 1 | Traffic filtering between the internal network and internet is updated and monitored regularly | ☐ | ☐ |
| 2 | Intrusion detection/prevention system is implemented, updated and monitored regularly | ☐ | ☐ |
| 3 | Internal users have access to Internet web site browsing through a network device (proxy) equipped with antivirus and website filtering | ☐ | ☐ |
| 4 | Network segmentation is implemented to separate critical areas from non critical areas | ☐ | ☐ |
| 5 | Penetration testing is conducted regularly and a remediation plan is implemented where necessary | ☐ | ☐ |
| 6 | Vulnerability assessments are conducted regularly and a remediation plan is implemented where necessary | ☐ | ☐ |
| 7 | Procedures for incident management and change management are implemented | ☐ | ☐ |
| 8 | Security events such as virus detection, access attempts, etc..., are logged and monitored regularly | ☐ | ☐ |
| **4.4 Physical security of computing room** | | **Yes** | **No** |
| 1 | Critical systems are placed in at least one dedicated computer room with restricted access and operational alarms are routed to a monitoring location | ☐ | ☐ |
| 2 | The data centre hosting critical systems has resilient infrastructure including | ☐ | ☐ |

| | | | |
|---|---|---|---|
| | redundancy of power supply, air conditioning, and network connections | | |
| 3 | Critical systems are duplicated according to Active/Passive or Active/Active architecture | ☐ | ☐ |
| 4 | Critical systems are duplicated on two separate premises | ☐ | ☐ |
| 5 | Fire detection and automatic fire extinguishing system in critical areas are implemented | ☐ | ☐ |
| 6 | The power supply is protected by a UPS and batteries which are both maintained regularly | ☐ | ☐ |
| 7 | Power is backed up by an electric generator which is maintained and tested regularly | ☐ | ☐ |

| **4.5 Outsourcing** | **Yes** | **No** |
|---|---|---|
| [Please fill in if a function of the information system is out sourced] | | |
| 1 The outsourcing contract includes security requirements that should be observed by the service provider | ☐ | ☐ |
| 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 | ☐ | ☐ |
| 3 Monitoring and steering committee(s) are organised with the service provider for the management and the improvement of the service | ☐ | ☐ |
| 4 You have not waived your rights of recourse against the service provider in the outsourcing contract | ☐ | ☐ |

| **What are the outsourced Information Systems functions?** | **Yes** | **No** | **Service Provider (Outsourcer)** |
|---|---|---|---|
| Desktop management | ☐ | ☐ | |
| Server management | ☐ | ☐ | |
| Network management | ☐ | ☐ | |
| Network security management | ☐ | ☐ | |
| Application management | ☐ | ☐ | |
| Use of cloud computing<br>If YES, please specify the nature of cloud services: | ☐ | ☐ | |
| Software as a Service | ☐ | ☐ | |
| Platform as a Service | ☐ | ☐ | |
| Infrastructure as a Service | ☐ | ☐ | |
| Other, to specify please: | | | |

| | | | |
|---|---|---|---|
| 5 | The outsourcing contract contains a provision requiring the service provider(s) to maintain professional indemnity or errors and omissions insurance | ☐ | ☐ |

## 5. Personal data held by the organization

### 5.1 Type and number of records

| | | | |
|---|---|---|---|
| The Number of personal information records held for the activity to be insured: | | | Total: |
| Per region: | Asia: | USA/Canada: | Hong Kong: |
| | Europe: | Australia: | Rest of the world: |

| Categories of personal data collected/processed | Yes | No | Number of records |
|---|---|---|---|
| Commercial and marketing information | ☐ | ☐ | |
| Payment Card or financial transactions information | ☐ | ☐ | |
| Health information | ☐ | ☐ | |

| | | | | |
|---|---|---|---|---|
| Other, to specify please: | | | | |
| Do you process data for: | ☐ | your own purpose? | ☐ | On behalf of third party? |

| | 5.2 Personal information protection policy | Yes | No |
|---|---|---|---|
| 1 | A privacy policy is formalised and approved by management and/or personal data security rules are defined and communicated to the concerned staff<br>If yes, please attached the copy of privacy policy | ☐ | ☐ |
| 2 | Awareness and training are provided at least annually to the personnel authorised to access or process personal data | ☐ | ☐ |
| 3 | A personal data protection officer is designated in your organisation | ☐ | ☐ |
| 4 | A confidentiality agreement or a confidentiality clause in the employment contract is signed by the concerned staff | ☐ | ☐ |
| 5 | The legal aspects of the privacy policy are validated by a lawyer/legal department | ☐ | ☐ |
| 6 | Monitoring is implemented to ensure compliance with laws and regulations for the protection of personal data | ☐ | ☐ |
| 7 | Your personal information practices have been audited by an external auditor within the past two years | ☐ | ☐ |
| 8 | A Data Breach Response plan is implemented and roles are clearly communicated to the functional team members<br>If yes, please attached the copy of Data Breach Response plan | ☐ | ☐ |

| | 5.3 Collection of personal data | Yes | No |
|---|---|---|---|
| 1 | If so required by any Privacy Protection Law, you have notified to the appropriate privacy protection agencies the personal data processing involved by your company and you have obtained the applicable authorization<br>Please explain if not applicable. | ☐ | ☐ |
| 2 | A privacy policy is posted on your website which has been reviewed by a lawyer/legal department | ☐ | ☐ |
| 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 | ☐ | ☐ |
| 4 | Recipients are provided with a clear means to opt out of targeted marketing operations | ☐ | ☐ |

| | | | |
|---|---|---|---|
| 5 | You transfer Personal Data to third parties<br>If YES. please answer the following: | ☐ | ☐ |
| 5.a | The third party (e.g processor) has a contractual obligation to process personal data only on your behalf and under your instructions | ☐ | ☐ |
| 5.b | The third party has a contractual obligation to set up sufficient security measures to protect personal data | ☐ | ☐ |

| **5.4 Personal information protection controls** | | **Yes** | **No** |
|---|---|---|---|
| 1 | Access to personal data is restricted to only those users who need it to perform their task and access authorizations are reviewed regularly | ☐ | ☐ |
| 2 | Personal data is encrypted when stored on information systems and personal data backups are encrypted | ☐ | ☐ |
| 3 | Personal data is encrypted when transmitted over the network | ☐ | ☐ |
| 4 | Mobile devices and laptop hard disks are encrypted | ☐ | ☐ |
| 5 | IS policy prohibits the copying of non-encrypted personal data to removable storage devices ortransmitting such data via email | ☐ | ☐ |

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:** |
|---|---|---|---|---|

| | **Yes** | **No** |
|---|---|---|
| The payment processor (yourself or third party) is PCI DSS compliant<br>If NO : | ☐ | ☐ |
| PCI is stored encrypted or only a part of payment card numbers is stored | ☐ | ☐ |
| PCI retention time does not exceed the duration of payment and legal/regulatory requirements | ☐ | ☐ |
| Payment card data processing is externalized , If YES: | ☐ | ☐ |
| You require the payment processor to indemnify you in case of security breach | ☐ | ☐ |

Please indicate payment processor name, PCI retention time and any additional security measures :

## 5.5 Incidents

[Please provide a description of any information security or privacy incidents that have occurredin the last 36 months. Incidents include any unauthorized 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 |
|---|---|
| Comment | |

NO person or entity proposed for cover is aware of any fact, circumstance or situation which he or she has reason to suppose might give rise to any claim that would fall within the scope of the proposed coverage.

| None☐ | or, except: |
|---|---|

Person to contact for additional information

| Name: | |
|---|---|
| Title: | |
| Phone: | |
| E-mail: | |
| Completed by: | |

## Declaration

- We acknowledge that we have read and understood the Important Notices contained in this proposal.
- 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 the Insurer.
- We declare after enquiry that the statements, particulars and information contained in this proposal and in any documents accompanying this proposal are true and correct in every detail and that no other material facts have been misstated, suppressed or omitted.
- We undertake to inform the Insurer of any material alteration to those facts before completion of the contract of insurance/insurance policy period (if applicable).

## Commission Disclosure

The following clauses should be added to Chubb's formal proposals / application forms/ quotations in order to obtain the clients' informed consent:

Disclosure:
The applicant understands, acknowledges and agrees that, as a result of the applicant purchasing and taking up the policy to be issued by Chubb Insurance Hong Kong Limited (Chubb), Chubb will pay the authorized insurance broker commission during the continuance of the policy including renewals, for arranging the said policy. Where the applicant is a body corporate, the authorized person who signs on behalf of the applicant further confirms to Chubb that he or she is authorized to do so.

The applicant further understands that the above agreement is necessary for Chubb to proceed with the application.

## Personal Information Collection Statement

**The Company** ("**We/Us**") want to ensure that Our **Insured Persons** ("**You**") are confident that any personal data collected by **Us** is treated with the appropriate degree of confidentiality and privacy.

This Personal Information Collection Statement sets out the purposes for which **We** collect and use personally identifiable information provided by **You** ("**Personal Data**"), the circumstances when **Personal Data** may be disclosed and information regarding Your rights to request access to and correction of **Personal Data**.

**(a) Purposes of Collection of Personal Data**

**We** will collect and use **Personal Data** for the purposes of providing competitive insurance products and services to **You**, including considering Your application(s) for any new insurance policies and administering policies to be taken out with **Us**, arranging the cover and administering and managing Your and Our rights and obligations in relation to such cover. **We** also collect the **Personal Data** to be able to develop and identify products and services that may interest **You**, to conduct market or customer satisfaction research, and to develop, establish and administer alliances and other arrangements with other organisations in relation to the promotion, administration and use of Our respective products and services. **We** may also use your **Personal Data** in other ways with your consent.

**(b) Direct marketing**

Only with your consent, **We** may also use your contact, demographic, policy and payment details to contact **You** with marketing information regarding our insurance products by mail, email, phone or SMS.

**(c) Transfer of Personal Data**

Personal Data will be kept confidential and **We** will not sell Your **Personal Data** to any third party. **We** limit the disclosure of Your **Personal Data** but, subject to the provisions of any applicable law, Your **Personal Data** may be disclosed to:

(i) third parties who assist **Us** to achieve the purposes set out in paragraphs a and b above. For example, **We** provide it to Our relevant staff and contractors, agents and others involved in the above purposes such as data processors, professional advisers, loss adjudicators and claims investigators, doctors and other medical service providers, emergency assistance providers, insurance reference bureaus or credit reference bureaus, government agencies, reinsurers and reinsurance brokers (which may include third parties located outside Hong Kong);
(ii) Our parent and affiliated companies, or any company within Chubb local and outside Hong Kong;
(iii) the insurance intermediary through which **You** accessed the system;
(iv) provided to others for the purposes of public safety and law enforcement; and
(v) other third parties with your consent.

With regard to the above transfers of **Personal Data**, where applicable, **You** consent to the transfer of Your **Personal Data** outside of Hong Kong.

**(d) Access and correction of Personal Data**

Under the **Personal Data** (Privacy) Ordinance ("PDPO"), **You** have the right to request access to and correction of **Personal Data** held by **Us** about **You** and **We** will grant **You** access to and correct Your **Personal Data** as requested by **You** unless there is an applicable exemption under the PDPO under which **We** may refuse to do so. **You** may also request **Us** to inform **You** of the type of **Personal Data** held by **Us** about **You**.

Requests for access or correction of **Personal Data** should be addressed in writing to:
Chubb Data Privacy Officer
39/F, One Taikoo Place,
979 King's Road,
Quarry Bay, Hong Kong
O +852 3191 6222
F +852 2519 3233
E Privacy.HK@chubb.com

Your request to obtain access or correction will be considered within forty (40) days of Our receipt of Your request. **We** will not charge **You** for lodging a request for access to Your **Personal Data** and if **We** levy any charges for providing information, such charges will not be excessive. No fee is charged for data correction requests.

| **Signature** | |
|---|---|
| Applicant's Signture | Applicant Name: |
| Date (DD/MM/YY): | Position: |

## About Chubb in Hong Kong SAR

Chubb is the world's largest publicly traded property and casualty insurer. With both general and life insurance operations, Chubb has been present in Hong Kong SAR for more than 90 years via acquisitions by its predecessor companies. Its general insurance operation in Hong Kong SAR (Chubb Insurance Hong Kong Limited) is a niche and specialist general insurer. The company's product offerings include property, casualty, marine, financial lines and consumer lines designed for large corporates, midsized commercial & small business enterprises as well as retail customers. Over the years, it has established strong client relationships by offering responsive service, developing innovative products and providing market leadership built on financial strength.

More information can be found at www.chubb.com/hk.

## Contact Us

Chubb Insurance Hong Kong Limited
39/F, One Taikoo Place,
979 King's Road,
Quarry Bay, Hong Kong
O +852 3191 6800
F +852 2560 3565
www.chubb.com/hk

Chubb. Insured.™