CHUBB®

Cyber ERM Proposal Form

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:

City: **Post code:**

Website(s):

Number of employees:	**Annual Turnover:**	**Annual Gross Margin:**

Percentage of turnover generated from:

UK/I:	**USA/Canada:**
Europe (EU):	**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 the UK, please provide the details]

CHUBB®

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
Počet uživatelů informačních systémů	☐	☐	☐
Počet notebooků	☐	☐	☐
Počet serverů	☐	☐	☐

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 actual)

4. Information security (IS)

4.1 Security policy and risk management

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
2	Formalised awareness training on the IS is required of all staff at least annually	☐ Yes	☐ No
3	You identify critical information systems risks and implement appropriate controls to mitigate them	☐ Yes	☐ No
4	Regular audits of the IS are conducted and resulting recommendations are prioritised and implemented	☐ Yes	☐ No
5	Information resources are inventoried and classified according to their criticality and sensitivity	☐ Yes	☐ No
6	Security requirements that apply to information resources are defined according to classification	☐ Yes	☐ No

4.2 Information systems protection

1	Access to critical information systems requires dual authentication	☐ Yes	☐ No
2	Users are required to regularly update passwords	☐ Yes	☐ No
3	Access authorisations are based on user roles and a procedure for authorisation management is implemented	☐ Yes	☐ No
4	Secured configurations references are defined for workstations, laptops, servers and mobile devices	☐ Yes	☐ No
5	Centralised management and configuration monitoring of computer systems are in place	☐ Yes	☐ No
6	Laptops are protected by a personal firewall	☐ Yes	☐ No
7	Antivirus software is installed on all systems and antivirus updates are monitored	☐ Yes	☐ No
8	Security patches are regularly deployed	☐ Yes	☐ No

CHUBB®

9	A Disaster Recovery Plan is implemented and updated regularly	☐ Yes	☐ No
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

1	Traffic filtering between the internal network and internet is updated and monitored regularly	☐ Yes	☐ No
2	Intrusion detection/prevention system is implemented, updated and monitored regularly	☐ Yes	☐ No
3	Internal users have access to Internet web site browsing through a network device (proxy) equipped with antivirus and website filtering	☐ Yes	☐ No
4	Network segmentation is implemented to separate critical areas from non critical areas	☐ Yes	☐ No
5	Penetration testing is conducted regularly and a remediation plan is implemented where necessary	☐ Yes	☐ No
6	Vulnerability assessments are conducted regularly and a remediation plan is implemented where necessary	☐ Yes	☐ No
7	Procedures for incident management and change management are implemented	☐ Yes	☐ No
8	Security events such as virus detection, access attempts, etc..., are logged and monitored regularly	☐ Yes	☐ No

4.4 Physical security of computing room

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
2	The data centre hosting critical systems has resilient infrastructure including redundancy of power supply, air conditioning, and network connections	☐ Yes	☐ No
3	Critical systems are duplicated according to Active/Passive or Active/Active architecture	☐ Yes	☐ No
4	Critical systems are duplicated on two separate premises	☐ Yes	☐ No
5	Fire detection and automatic fire extinguishing system in critical areas are implemented	☐ Yes	☐ No
6	The power supply is protected by a UPS and batteries which are both maintained regularly	☐ Yes	☐ No
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]

1	The outsourcing contract includes security requirements that should be observed by the service provider	☐ Yes	☐ No
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
3	Monitoring and steering committee(s) are organised with the service provider for the management and the improvement of the service	☐ Yes	☐ No
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?			**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	☐ Yes	☐ No		
	If yes, please specify the nature of cloud services:				
	Software as a Service	☐ Yes	☐ No		
	Platform as a Service	☐ Yes	☐ No		
	Infrastructure as a Service	☐ Yes	☐ No		
	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			☐ Yes	☐ No

5. Personal data held by the organisation

5.1 Type and number of records

The Number of personal information records held for the activity to be insured:

Total:

Per region:

UK/I:	**USA/Canada:**
Europe (EU):	**Rest of the world:**

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	
Other, to specify please:			

Do you process data for: ☐ your own purpose? ☐ On behalf of third party?

5.2 Personal information protection policy

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
2	Awareness and training are provided at least annually to the personnel authorised to acces or process personal data	☐ Yes	☐ No
3	A personal data protection officer is designated in your organisation	☐ Yes	☐ No
4	A confidentiality agreement or a confidentiality clause in the employment contract is signed by the concerned staff	☐ Yes	☐ No
5	The legal aspects of the privacy policy are validated by a lawyer/legal department	☐ Yes	☐ No
6	Monitoring is implemented to ensure compliance with laws and regulations for the protection of personal data	☐ Yes	☐ No
7	Your personal information practices have been audited by an external auditor within the past two years	☐ Yes	☐ No
8	A Data Breach Response plan is implemented and roles are clearly communicated to the functional team members	☐ Yes	☐ No

CHUBB®

5.3	Collection of personal data		
1	You have notified to the Data Protection Authority (DPA) the personal data processing involved by your company and you have obtained the applicable DPA authorization Please explain if not applicable	☐ Yes	☐ No
2	A privacy policy is posted on your website which has been reviewed by a lawyer/ legal department	☐ Yes	☐ No
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
4	Recipients are provided with a clear means to opt out of targeted marketing operations	☐ Yes	☐ No
5	You transfer Personal Data to third parties 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		
1	Access to personal data is restricted to only those users who need it to perform their task and access authorizations are reviewed regularly	☐ Yes	☐ No
2	Personal data is encrypted when stored on information systems and personal data backups are encrypted	☐ Yes	☐ No
3	Personal data is encrypted when transmitted over the network	☐ Yes	☐ No
4	Mobile devices and laptop hard disks are encrypted	☐ Yes	☐ No
5	IS policy prohibits the copying of non encrypted personal data to removable storage devices or transmitting such data via emailtransmission	☐ Yes	☐ No

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

(please refer to definitions page at the end of this document)

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

Payment card data processing is externalized	☐ 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 :

CHUBB®

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:	

I/we declare that I/we have made a fair presentation of the risk, by disclosing all material matters which I/we know or ought to know or, failing that, by giving the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material circumstances.

Signatory Name and surname	Function
Date	Signature

Chubb. Insured.℠