Chubb Assembly

Public/Product Liability, Manufacturers E&O Liability and Cyber Enterprise Risk Management

Proposal Form

For the purposes of this proposal form, "we", "us", "our" and "Chubb" means Chubb Insurance Singapore Limited.

Important Notices to the Applicant

You must fully and faithfully disclose all facts which you know or ought to know, including n this Proposal Form, otherwise the policy may be void.

1) Your Duty of Disclosure
Before you enter into a contract of general insurance with an insurer, you have a duty under the law 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. If you are unsure whether a matter is material, you should disclose it. 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 application 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.

2) Consequences of Non-Disclosure
If you fail to comply with your duty of disclosure Chubb may be entitled, without prejudice to its other rights, to reduce its liability under the contract in respect of a claim or refuse to pay the entire claim. Chubb may also have the right to avoid the contract from its beginning. This means the contract will be treated as if it never existed and no claims will be payable.

3) Claims Made And Claims Made And Notified Coverages
If your policy, or a part of your package policy, provides cover on a claims made or claims made and notified basis, the following will apply, but not otherwise.

These coverages apply only to claims that are either first made against you during the period of insurance or both first made against you and notified to us in writing before the expiration of the period of the insurance cover provided by your policy. If your policy does not have a continuity of cover provision or provide retrospective cover then your policy may not provide insurance cover in relation to events that occurred before the contract was entered into.

4) Change of Risk or Circumstances
There is the same duty to disclose material information to Chubb before renewal, extension, variation or reinstatement of a contract of insurance with Chubb. You should also provide all material information when you make a claim or if circumstances change during the term of the contract of insurance, such as changes in business activities, location, acquisitions and new overseas activities.

5) 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, the Insurer will not cover you, to the extent permitted by law, for such loss or damage.

Instructions to the Applicant

Completing the Proposal Form:

- Please note that this proposal form is being completed by the Applicant on behalf of all the Named Insureds to be covered and as defined in the policy. Whenever used in this proposal form, the terms 'You' and 'Your' shall mean the Named Insured and all of its Subsidiaries.
- Please read the Important Notices on pages 1 - 2.
- Please answer all questions. If you have insufficient space to complete any of your answers, please attach a separate signed and dated sheet and identify the question number concerned.
- For all words in BOLD Green, please refer to the definition in the Glossary of Defined Terms on page 10.

I. Company Information

Applicant: (please also list all subsidiary companies and your parent company, if applicable)

Principal Address (Street, City & Country): *please attach list of locations, if more than one*

Year Established		Website URL	
Do you have a subsidiary, affiliate or representative office in the USA/ Canada?		☐ Yes ☐ No If yes, please provide the details below.	
Name of Company		USA/Canada Address	
Number of Employees		Business Nature in USA/Canada	

II. Limit of Insurance

1. Please provide details of your current insurance policies (if applicable) (please specify currency)

Coverage	Limit	Deductible	Premium	Insurer	Retroactive Date (MM/DD/YYYY)
Public Liability					
Product Liability					
Manufacturer Error and Omission					
Cyber Enterprise Risk Management					

2. Please indicate the Limit of Insurance for which you would like to receive a quote (please specify currency)

	Limit	Deductible
Public Liability		
Product Liability		
First and Third Party Product Recall Expenses		
Manufacturing Errors and Omissions Liability		
Cyber Enterprise Risk Management		

III. Turnover

Please complete the table below to reflect your global turnover (please specify currency)

Territory	Estimated Forthcoming Year	Current Year	Prior Year
Domestic			
USA/Canada Domestic			
USA/Canada Exports			
Rest of World			
Total			

IV. Activities

1. Business Activities

Please provide a clear description of the insured products and services, including all work performed by subsidiary companies:

a. How many years have you been manufacturing/ producing this product(s)?

b. Please confirm if your products are:	☐ End Products ☐ Components, please advise the application for the end product
c. What percentage of your product are:	☐ Designed by you only ____ % ☐ Designed and Manufactured by you ____ % ☐ Manufactured to customer specification ____ % ☐ Others ____ %

2. Turnover by Products

Please list all the products that are manufactured, processed, assembled or distributed by you and indicate the approximate percentage of turnover from each product.

Type of Product	**Forthcoming Year (%)**	**Current Year (%)**

(Please continue on a separate sheet of paper if insufficient space)

3. Acquisitions

Have you made any acquisitions in the past 3 years?	☐ Yes ☐ No

If **Yes**, please provide a description including details of any past liabilities you acquired.

4. Financial Results	
Over the past 4 years, in how many years did you post a positive net income	☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4

V. Quality Controls

1. Do you have a written and formalised quality control program?	☐ Yes ☐ No
2. Do you have a formal procedure for documenting problems, downtime, and responding to customer complaints and feedback?	☐ Yes ☐ No
3. What industry standards do you work with in the delivery of your products and services? Please list below. ☐ ISO9001 ☐ Member of ICTI ☐ GMP ☐ HACCP ☐ Others (please specify)	
4. If you manufacture or have a third-party manufacture on your behalf, do you, or a third-party manufacturing on your behalf, have quality control procedures such as: • Written and formalised quality control plan or programme • Production design sign off acceptance and sign off procedures for statements of work or contracts • Prototype development protocols • Batch testing	☐ Yes ☐ No
5. Do you have a Product Recall Plan or Procedures in place? If yes, please provide details or copy of procedures.	☐ Yes ☐ No
6. Are generic notification letters, media alerts or safety hazard notices prepared and/or available for delay-free implementation in the event of a recall?	☐ Yes ☐ No
7. Do you have a formal procedure to trace all products and batches?	☐ Yes ☐ No
8. Are all products coded by date, batch, company and product type?	☐ Yes ☐ No
9. Please describe your typical batch size (please specify currency).	$ ☐ ☐ units
10. Are deliveries of raw material, components or products done on a regular basis (weekly, monthly etc.)?	☐ Yes ☐ No
11. Do you maintain distribution, sales and inventory control record for a minimum of ten (10) years?	☐ Yes ☐ No
12. How much inventory do you keep on site for normal production runs?	☐ weeks
13. Do you operate or publish a consumer complaint service or hotline?	☐ Yes ☐ No

14. Please advise mode of sales distribution:

☐ Direct to Public ☐ Third Party Sales ☐ Field Sales (Sales Reps)
☐ E-Commerce ☐ Wholesales ☐ Others

VI. Manufacturing Errors and Omissions

Contract and Risk Management

1. Please detail your five largest contracts in the past three years.

Client Name	Nature of Work Description	Total Contract Value
		$
		$
		$
		$
		$

2. Please provide copies of your standard and largest sales, service and license contracts, agreements, or purchase orders.

☐ Standard and Written	% of the time	☐ Custom Contract	% of the time
☐ Purchase Order	% of the time	☐ Verbal Contract	% of the time
☐ Invoice	% of the time	☐ Other	% of the time

3. What is the value of your average contract, agreement or purchase order? (US$)

4. Do you negotiate contracts or agreements in which you accept liability for consequential damages, except Intellectual Property? ☐ Yes ☐ No — % of the time

5. Do all your contracts or agreements limit your liability to the cost of your product or service? ☐ Yes ☐ No

6. Do you perform legal review of all standard contracts and marketing materials prior to release? ☐ Yes ☐ No

7. In what percentage of contracts do you cap your liability?

Below contract value	%	At contract value	%	More than contract value	%

Subcontractors and Suppliers

1. What percentage of your annual turnover will be subcontracted to others? %

2. Please describe the work that you subcontract to others:

3. Do you require subcontractors and suppliers to carry product liability insurance? ☐ Yes ☐ No

4. Do you maintain full subrogation rights against your subcontractors and suppliers? ☐ Yes ☐ No

Consequential Loss

1. Please select the likely result of a failure of your products or services or delay in their implementation. *Choose all that apply.*

☐ Loss of life or injury	☐ Immediate and large financial loss	☐ Damage or destruction of property
☐ Minor disruption or delayed impact	☐ No disruption	

Please provide detail for any selected items above:

VII. Cyber Enterprise Risk Management

Data Privacy

1. Approximately how many unique individuals and organisations would you be required to notify in the event of a breach of Personally Identifiable Information (PII)?	
2. Which of the following types of **Sensitive Records** do you store, process, transmit or otherwise have responsibility for securing?	
a. Customers and business partners confidential information	☐ Yes ☐ No
b. Employee information	☐ Yes ☐ No
c. Personal Information (name, address)	☐ Yes ☐ No
d. TFN, Driving licence Passport or other ID	☐ Yes ☐ No
e. Healthcare or medical records	☐ Yes ☐ No
f. Biometric information (If yes see Appendix)	☐ Yes ☐ No
g. Credit card numbers, debit card numbers or other financial account numbers	☐ Yes ☐ No
3. Is any payment card information processed in the course of your business?	☐ Yes ☐ No
If **Yes**, please indicate the level of **PCI DSS** compliance	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ Not Compliant

Intellectual Property and Media

1. Do you Maintain Forums or Social Media	☐ Yes - Active Management ☐ Yes - Passive Management ☐ No
2. Do you have Clearance Procedures for any publication	☐ Yes ☐ No

Data and Information Security

1. Please detail if you comply with or adhere to any internationally recognised cyber security or information governance standards:

2. Which of the following have you (or your provider, if outsourced) implemented to help protect information and systems from a **Data Breach** or a **Cyber Incident**?

Governance

☐ Dedicated staff member governing data security	☐ Dedicated staff member governing IT security	☐ Ongoing staff training on cyber-related matters
☐ Use of **Threat Intelligence**	☐ Ransomware event and recovery plan	☐ Security policy and annually reviewed
☐ Vulnerability patching policy	☐ Formal privacy policy approved by legal counsel and management	☐ Maintain compliance with all applicable **privacy laws and regulations**, including GDPR, HIPPA, NBD or others
☐ Formal information security policy approved by legal counsel and management	☐ Formal data classification policy	☐ Formal data retention policy
☐ Formal **Data Breach** response plan that is tested at least annually	☐ **Privileged Accounts** controlled by a **Privileged Access Management (PAM)** solution	

Protections		
☐ Firewalls & Antivirus	☐ Vulnerability scans	☐ **Intrusion Detection Systems**
☐ **Encryption** of data in transmission	☐ **Encryption** of data in use and at rest	☐ **Sandboxing** Technology to test new software
☐ **Security Information and Event Monitoring (SIEM)** tool	☐ External penetration testing at least annually	

Do you allow remote access to your corporate network or operational technology environment?	☐ Yes ☐ No

Please confirm **Multi-Factor Authentication (MFA)** in place on the following:

☐ Remote Email	☐ Remote Access	☐ Internal Admin and **Privileged Accounts**
☐ **Remote Desktop Protocol (RDP)**		

Please confirm the Endpoint protections in place from the following:

☐ Anti-malware and anti-virus with **Heuristic Analysis**	☐ **URL Filtering or Web Filtering**	☐ Application Isolation and containment
☐ **Endpoint Detection and Response (EDR)** tool	☐ **Extended Detection and Response (XDR)** tool	☐ **Managed Detection and Response (MDR)** tool

Please confirm the Email Security controls in place from the following:

☐ Quarantine of suspicious Email	☐ **Sandbox** detonation of attachment/links	☐ Sender policy framework
☐ Microsoft Office macros disabled	☐ Annual phishing simulation	

Business Interruption and Data and System Recovery			
Business Continuity Plan (BCP)	☐ Yes - tested regularly	☐ Yes - not tested	☐ No
Disaster Recovery Plan (DRP)	☐ Yes - tested regularly	☐ Yes - not tested	☐ No
Cyber Incident Response Plan (IRP)	☐ Yes - tested regularly	☐ Yes - not tested	☐ No

Please detail which of the following protections you have in place for mission critical backups:

☐ Mission Critical Backup Protection	☐ Specifically tested and prepared for as part of disaster recovery planning	☐ Test for recoverability as well as integrity
☐ Immutable or **Write Once Read Many (WORM)** back up technology	☐ Restricted access via **MFA**	☐ Fully Encrypted

☐ Completely **Offline** or **Air-Gapped** (tape/non-mounted disks) backups that are disconnected from the rest of the network

☐ Others (please describe)				
Data Backups	☐ Daily	☐ Weekly	☐ Less than weekly	
Data Segmentation	☐ Business Segment	☐ Contract or customer	☐ Geography	☐ Critical and Non-critical
Critical System Backups	☐ Daily	☐ Weekly	☐ Less than weekly	

Please detail which of the following alternative systems you have in place for critical applications?

☐ Automatic failover (Active - Active)	☐ Automatic failover (Active - Passive)	☐ Manual failover
☐ Colocation facility	☐ Offline alternative environment	☐ Alternative provider (if outsourced)
☐ Others (please describe)		

Systems

1. Do you use any end-of-life or unsupported hardware, software or systems?	☐ Yes ☐ No

2. **Criticality of Information Systems** – please describe the systems on which you depend most to operate your business (including **Outsourced Technology Providers**), and the impact downtime of each would have.

IT Provider (if not outsourced, put "Internal")	IT Application or Activity	**Recovery Time Objective (RTO)**			
		Immediate	>12 hours	>24 hours	Other
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐

a. Do you perform assessments or audits to ensure third party technology providers meet your company's security requirements?	☐ Yes ☐ No
b. Do you waive your right of recourse against any of the providers listed above in the event of service disruption?	☐ Yes ☐ No

Operational Technology Exposure Information

1. Do you use any **Operational Technology**?	☐ Yes ☐ No

2. Do the responses on the proposal form apply equally to operational / Shop floor technology as to information technology?

3. How is Operational Technology secured and patching maintained? Particularly, how is patch management implemented? Is any patching process tested outside of the operational environment before being deployed?

4. Are all production lines and their associated operational technology systems segmented from each other?

5. Are any operational technology systems or production line technology accessible via remote access? Are these systems connected to the internet at any time? If yes, what are the access controls for such connectivity and what additional security is applied around such access points?

6. Is a unique power supply and or back-up generator(s) used for each production line? How often are these back-up systems tested and maintained?

7. If the production lines were stopped or impeded by malicious software how long would it take to reboot the lines and return to full production? What are the Recovery Time Objectives (RTO's) of the organisation?

8. What is the average value of any Work in Process (WIP) for a production month?

9. Highlight the redundancy processes that are in place to mitigate any operational technology / product line outage?

10. What are the access controls to the production line / operational technology systems? Is multi factor authentication required?

11. Do they have redundant rooms or facilities, capability to operate in isolation and are these centrally controlled or locally controlled?

VIII. Loss History

1. Have you ever experienced any actual or potential Public and Product Liability Claims, Recall Claims, **E&O Claims**, **Media Claims**, **Data Breaches**, or **Cyber Incidents** in the past three years?	☐ Yes ☐ No

If **Yes**, please provide:

Description of any claims/incidents and date of occurrence:

Description of the financial impact:

Mitigating steps you've taken to avoid similar future events:

2. Are you aware of any notices, facts, circumstances, or situations which may give rise to any Public and Product Liability Claims, **E&O Claims**, **Media Claims**, **Data Breaches**, or **Cyber Incidents**?	☐ Yes ☐ No

If **Yes**, please provide additional details:

3. Please advise if there has ever been any voluntary or mandatory recall of any of your products?	☐ Yes ☐ No

If **Yes**, please provide additional details:

IX. Data Protection

You consent and confirm that you have obtained the consent of the individual(s) whose information is shared, for Chubb to collect, use, disclose, and process the information in accordance with our Privacy Notices. This may include sharing the information with parties mentioned in the policy, some of which may be located outside of Singapore. To learn more, please visit www.chubb.com/sg-privacy.

X. Declaration

I/We (the undersigned):

a) acknowledge that we have read and understand the Important Notices and Data Protection sections contained in this Proposal Form;

b) agree that this proposal, together with any other information or documents supplied, shall form the basis of any resulting contract of insurance;

c) acknowledge that if this application 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;

d) 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;

e) undertake to inform Chubb of any material alteration to those facts before completion of the contract of insurance

Name of Director, Officer, or Risk Manager	Signature	Date

Please enclose with this proposal form:

☐ Product Photos ☐ Lab Test Report in respect of product safety ☐ QC Certificate

☐ A copy of your standard contract template ☐ A copy of your largest active, non-standard contract

Glossary of Defined Terms

Advanced Endpoint Protection is a device or software that provides protects and monitors the endpoints on your network. Endpoints include desktop and laptop computers, tablets, mobile phones, servers, and any other device connected to your network.

Cyber Incident includes unauthorised access to your computer systems, hacking, malware, virus, cyber extortion, distributed denial of service attack, insider misuse, human or programming error, or any other cyber-related event.

Data Breach defined as "An incident where sensitive personal or corporate confidential information has been taken, lost, or viewed by an unauthorised party."

An **E&O Claim** includes any failure of your product or service that's provided to any of your customers, resulting in a financial loss.

Encryption is the method of converting data from a readable format to an encoded format. It can only become readable again with the associated decryption key.

Endpoint Detection and Response (EDR) is a solution which records and stores endpoint-system-level behaviours, use various data analytics techniques to detect suspicious system behaviour, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems.

Extended Detection and Response (XDR) is a security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components, typically including endpoints, networks, servers, cloud services, SIEM, and more.

Heuristic Analysis looks for suspicious properties
in code, going beyond traditional signature-based detection in basic antivirus software, and can determine the susceptibility of a system towards particular threat using various decision rules or weighing methods designed to detect previously unknown computer viruses, as well as new variants of viruses already in the "wild".

An **Intrusion Detection System** is a device or software that monitors your network for malicious activity or policy violations.

Managed Detection and Response (MDR) is a managed cyber security service that provides intrusion detection of malware and malicious activity in your network, and assists in rapid incident response to eliminate those threats with succinct remediation actions.

Media Claim includes any claim for product disparagement, slander, trade libel, false light, plagiarism, or similar from your website or social media accounts.

Multi-Factor Authentication (MFA) is an electronic authentication method used to ensure only authorised individuals have access to specific systems or data. A user is required to present two or more factors - these factors being 1) something you know, 2) something you have, or 3) something you are. Something you know may include your password or a pin code. Something you have may include a physical device such as a laptop, mobile device that generates a unique code or receives a voice call or a text message, a security token (USB stick or hardware token), or a unique certificate or token on another device. Something you are may include biometric identifiers.
Note that the following are not considered secure second factors: a shared secret key, an IP or MAC address, a VPN, a monthly reauthentication procedure, or VOIP authentication.

Offline or Air-gapped relates to backup solutions, offline or air-gapped storage means that a copy of your data and configurations are stored in a disconnected environment that is separate to the rest of your network. Physical tape or non-mounted disk backups that aren't connected to the internet or LAN would be considered offline.

Operational Technology is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. Operational Technology may include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), robotics systems, and more.

Outsourced Technology Partners include cloud services, website hosting, collocation services, managed security services, broadband ASP services, outsourced services, internet communications services, credit card processing, anti-virus software, firewall technology, intrusion detection software and other providers such as human resources, payroll, point of sale.

PCI DSS stands for the Payment Card Industry Data Security Standard. This defines the requirements that a company must comply with if they handle any payment card information.

Privacy Laws and Regulations describes the body of law that sets the requirements and regulations for the collection, storage, and usage of personally identifiable information, personal healthcare information, financial information of individuals, and other sensitive data which may be collected by public or private organisations, or other individuals.

Privileged Access Management (PAM) describes enterprise processes and technology supporting Privileged Accounts. PAM solutions offer an additional layer of protection, and typically have automated password management, policy enforcement capabilities, account lifecycle management capabilities, as well as monitoring and reporting of privileged account activity.

Privileged Account means accounts that provide administrative or specialised levels of access based on a higher level of permission.

Recovery Time Objective (RTO) is the amount of real time a business has to restore its processes at an acceptable service level after a disaster to avoid intolerable consequences associated with the disruption.

Remote Desktop Protocol (RDP) is a Microsoft protocol that allows for remote use of a desktop computer.

Sandboxing relates to email solutions, a sandbox filters emails with unknown URL links, attachments, or other files, allowing them to be tested in a separate and safe environment before allowing them to proceed to your network or mail servers.

Security Information and Event Monitoring (SIEM) is technology and related services that provide real-time analysis of cyber security alerts from a collection of sources, including endpoints and applications to allow for improved detection, compliance enforcement, and incident management.

Sensitive Records include health or medical records of employees or customers, government issued identification numbers, usernames and passwords, email addresses, credit card numbers, intellectual property, or any other personally identifiable information.

Threat Intelligence is information on current security threats, vulnerabilities, targets, bad-actors, and implications that can be used to inform security decisions.

URL Filtering or Web Filtering is technology that restricts which websites a user or browser can visit on their computer, typically filtering out known malicious or vulnerable websites.

Write Once Read Many (WORM) is a data storage device in which information, once written, cannot be modified.

Appendix

Biometric Information

1. Do you collect biometric information from:

a. Employees	☐ Yes ☐ No
b. Service Providers or Contractors	☐ Yes ☐ No
c. Customers	☐ Yes ☐ No
d. Others (please specify):	☐ Yes ☐ No

2. Regarding biometrics collected, used, or stored on employees:

a. Do you receive written consent and a release from each individual?	☐ Yes ☐ No
b. Do you require each employee to sign an arbitration agreement with a class action waiver?	☐ Yes ☐ No
3. Do you have formal written policies pertaining to biometric information privacy requirements that clearly addresses retention and destruction guidelines?	☐ Yes ☐ No
4. Is written consent always obtained, and is this explicit consent?	☐ Yes ☐ No
5. When did you start collecting, storing, or processing biometric data?	
6. How long have you had requirements for explicit written consent?	

7. Please detail how much biometric information records you hold or are responsible for:

Multinational Capabilities for Large Domestic and Global Businesses

We have capabilities to issue admitted policies overseas, including Property, General Liability, Professional Indemnity, Cyber, US Auto and Workers Compensation or Employers' Liability.

For the purposes of Chubb Assembly, we most commonly arrange local General Liability cover. Therefore, for all Territories where local paper is required (USA, UK, Canada etc.) please complete the below table with the local (overseas) entity information:

Country	Entity Name(s)	Address	Revenue	Employee Numbers	Wage Roll	Local Limit Required

About Chubb

Chubb is a world leader in insurance. With operations in 54 countries and territories, Chubb provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. The company is defined by its extensive product and service offerings, broad distribution capabilities, exceptional financial strength and local operations globally. Parent company Chubb Limited is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index. Chubb employs approximately 43,000 people worldwide. Additional information can be found at: www.chubb.com

Contact Us

Chubb Insurance Singapore Limited
Co Regn. No.: 199702449H
138 Market Street
#11-01 CapitaGreen
Singapore 048946
O +65 6398 8000
www.chubb.com/sg