CHUBB®

PremierClimate PI, Cyber and General Liability

Proposal Form

Completing This Proposal Form

- Please read the "Statutory Notice" before completing this proposal form.
- 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.
- It is agreed that whenever used in this proposal form, the terms 'You' and 'Your' shall mean the Named Insured and all of its Subsidiaries as those terms are defined in the PremierClimate Policy Wording.
- Items listed in blue are defined terms in Glossary of Defined Terms on page 12.

I. Company Information

1. Company Name (please also list all subsidiary companies and Your parent company, if applicable)

2. Principal Address					
3. Year Established					
4. Number of Locations	a. Total		b. USA only		
5. Number of Employees	a. Total		b. USA only		
	c. Technical Staff		d. Non-Technical Staff		
6. Website URL(s):					

II. Acquisitions

Have you made any acquisitions in the past 18 months?	☐ Yes ☐ No

a. If Yes, please provide a brief description below. Note that a supplementary form may be required.

III. Turnover

Please complete the table below to reflect Your global turnover:

Turnover	Prior complete financial year	Estimated current year	Estimated following year
Domestic	$	$	$
USA & Canada Domestic	$	$	$
USA & Canada Exports	$	$	$
Rest of World	$	$	$
Total	$	$	$

Installed Capacity

Year	Installed capacity (MW)	Number of projects
Prior complete financial year		
Estimated current year		
Estimated following year		

IV. Financial Results

Over the past 4 years, how many years did You record a positive net income?	☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4

V. Limit of Insurance

1. Please provide details of Your current insurance policies (if applicable)

Coverage	Limit	Excess	Premium	Insurer	Retroactive Date (DD/MM/YYYY)
Professional Liability	$	$	$		
Cyber	$	$	$		
General Liability	$	$	$		

2. Please indicate the limits for which You would like to receive a quote

Professional Liability (PI/E&O)	☐ $1m	☐ $2m	☐ $5m	☐ $10m	☐ Other, $
Cyber	☐ $1m	☐ $2m	☐ $5m	☐ Other, $	
General Liability	☐ $5m	☐ $10m	☐ $20m	☐ Other, $	

3. Please select Your desired excess:

Professional Liability (PI/E&O)	☐ $10,000	☐ $25,000	☐ $50,000	☐ $100,000	☐ Other, $
Cyber	☐ $10,000	☐ $25,000	☐ $50,000	☐ $100,000	☐ Other, $
General Liability	☐ $1,000	☐ $5,000	☐ $10,000	☐ Other, $	

VI. Activities

1. Business Activities

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

2. Turnover by Business Activity

a. Please categorise Your business activities and indicate the approximate percentage of turnover from each.

Type of Product or Service	%	Type of Product or Service		%
IT Services		Consulting		
Software Development		Project Management		
Sales/ Wholesale/ Distribution		Geotechnical & Soil Engineering		
Product Design		Environmental Engineering		
Contract Manufacture to Customer Specifications		Mechanical, Hydraulic, Plumbing, HVAC & Fire Engineering		
Original Equipment Manufacturer (OEM)		Chemical Engineering		
Electrical Engineering		Renewable Energy	Design	
Industrial Process Engineering			Design and Construction	
Civil Engineering			Operations and Maintenance	
Structural Engineering			Asset Management	

b. Please describe Your consulting activities, if any:

c. Please describe any planned changes to the nature or functionality of Your core products, services, or business strategy/activities in the next 12 months.

This should include any new projects or new customer segments that You anticipate servicing. If there are no planned changes, please put "none".

d. Please provide the percentage split of the type of work of Your end customers.

Type of work	%	Type of work	%
Government		Industrial	
Commercial		Utility company or SPV	
Residential			

e. Please describe the scope of products or services provided to the following areas, as well as the percentage of turnover from each.

Application of Products or Services	Description of Products or Services	% of Annual Turnover
Cybersecurity		
Oil, Gas, Thermal Power or Nuclear Utilities		
Trading Platforms/Online Exchanges / Cryptocurrency		
Mass/ Public Transportation		

f. What percentage of Your professional services work is:

Type of work	%
Feasibility studies	
Design only. with no construction phase responsibility	
Observation of construction only	
Design with supervisions of construction where construction is done by others	
Design and construct or turnkey projects	

VII. Contract and Risk Management

1. Please detail Your five largest contracts in the past three years, considering the following 3 contracts periods:

   #1 The Development Work period is that part of the deliverables & milestones noted in a contract relating to planning, design, build, development and testing but prior to deployment, transition, operation, maintenance or support.

   #2 Deployment period is the work period part in a contract relating to the time taken for installation or construction prior to it becoming operational.

   #3 Licence/Maintenance period means that part in a contract relating to the maintenance post it becoming operational.

Client	Description of work	Total Contract Value and Fees	Contract Dates (DD/MM/YYYY)	Design / Development Works (Value/months)	Construction / Deployment Period (Value/months)	Operation / Licence / Maintenance (Value/months)
			Start:	$	$	$
			End:	months	months	months
			Start:	$	$	$
			End:	months	months	months
			Start:	$	$	$
			End:	months	months	months

			Start:	$	$	$
			End:	months	months	months
			Start:	$	$	$
			End:	months	months	months

2.	Typical size of active contract	$ or MW
3.	Typical length of active contract	months
4.	What percentage of the time do You use Your standard contract template?	☐ Less than 50% ☐ Less than 80% ☐ More than 80%
5.	Does qualified legal counsel review all critical contracts, such as critical vendor contracts, boilerplate standard customer contracts, and any substantially customised or deviated contracts for larger customers?	☐ Yes ☐ No
6.	In what percentage of contracts do You cap Your liability?	

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

7.	Approximately what percentage of Your customer contracts, purchase orders, or user agreements contain:	
	Hold harmless or indemnity agreements insuring to the benefit of You?	☐ Less than 75% ☐ More than 75%
	Hold harmless or indemnity agreements insuring to the benefit of the customers?	☐ Less than 75% ☐ More than 75%
	Statement of work or description of services that You provide	☐ Less than 75% ☐ More than 75%
	Formalised change order processes requiring signoff by both parties?	☐ Less than 75% ☐ More than 75%
	Conditions for customer acceptance of products/services?	☐ Less than 75% ☐ More than 75%
	Exclusion of consequential damages?	☐ Less than 75% ☐ More than 75%
	Provisions for liquidated damages?	☐ Less than 75% ☐ More than 75%
	Provisions for the ownership of intellectual property?	☐ Less than 75% ☐ More than 75%
	A dispute resolution/arbitration process?	☐ Less than 75% ☐ More than 75%
	Limitation of liability provisions that extend to actual or alleged breach of **Sensitive Records**?	☐ Less than 75% ☐ More than 75%
8.	Have You taken on any contracts for projects that the customer previously terminated with another party? If Yes, please provide a description:	☐ Yes ☐ No

VIII. Subcontractors or Labour Hire

1.	What is the percentage of sub-contractors or labour hire You engage as a percentage of turnover?	%
2.	Please describe the tasks the third party sub-contractors or labour hire workers are used for:	
3.	What is the maximum number of third party labour hire staff on site at any one time?	
4.	Do You require subcontractors to carry professional indemnity insurance?	☐ Yes ☐ No
5.	Do You require subcontractors to carry workers compensation (WC) and public and product liability?	☐ Yes ☐ No
6.	Do You maintain full subrogation rights against Your subcontractors?	☐ Yes ☐ No

IX. Consequential Loss

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

☐ Loss of life or injury
☐ Damage or destruction of property
☐ Significant cumulative financial loss
☐ Immediate and large financial loss
☐ Insignificant loss

Please provide detail for any selected items above:

X. Quality Controls

1.	Do You have a formal procedure for documenting problems, downtime, and responding to customer complaints and feedback?	☐ Yes ☐ No

2. Please list any International Risk Management (i.e. ISO), Quality Assurance (i.e. HACCP, SQF) and or Good Manufacturing Practice programs You have in place.

ISO / HACCP / Testing Accreditation

3. What industry standards do You work with in the delivery of Your products and services? Please list below.

4. For development, construction and integration projects:

a.	Do You have development methodology in writing?	☐ Yes ☐ No
b.	Are there change control provisions to deal with changes and scope creep made and signed by both parties in writing?	☐ Yes ☐ No
c.	Is there a formal customer acceptance process upon delivery of Your projects, products and services?	☐ Yes ☐ No

5. 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:

a.	Formalised, written quality control plans	☐ Yes ☐ No
b.	Production design sign off procedures for statements of work or contracts	☐ Yes ☐ No
c.	Prototype development protocols	☐ Yes ☐ No
d.	Batch testing	☐ Yes ☐ No
6.	Do You have a formal product recall plan or procedures in place?	☐ Yes ☐ No
a.	Do You have a formal procedure to trace all products and batches?	☐ Yes ☐ No
b.	Are all products coded by date, batch, company and product type?	☐ Yes ☐ No
c.	Please describe Your typical batch size for a normal production run.	$ ____ / ____ units

XI. Intellectual Property and Media

1.	Do Your intellectual property protection or compliance procedures include the following:	
a.	Formal procedure to safeguard against infringing the intellectual property rights of others	☐ Yes ☐ No
b.	Searches conducted for all trademark, copyright and patent applications	☐ Yes ☐ No
c.	Release or consent sought from third party right owners where content is not Your own	☐ Yes ☐ No
d.	Legal counsel is consulted prior to release of all new products	☐ Yes ☐ No
e.	Legal counsel review of all content prior to publication	☐ Yes ☐ No
2.	What percentage of Your turnover is derived from Your own products or Your own software that are:	
a.	less than three years old	%
b.	three to five years old	%
c.	over five years old	%
3.	Do all new employees and "work for hire" contractors acknowledge that use of a previous employer's or client's intellectual property, know-how, and trade secrets is strictly prohibited?	☐ Yes ☐ No
4.	Have Your privacy policy, terms of use, terms of service and other customer policies been reviewed by legal counsel?	☐ Yes ☐ No

XII. Data and Information Security

1.	Please provide contact details for the client's CISO or other staff member who is responsible for data and network security:			
	Name: (first and surname)		Email	
	Role:		Phone	
2.	Are You a subsidiary, franchisee, or small entity of a larger/parent organisation?			☐ Yes ☐ No
a.	If yes, please provide details and answer the following questions:			
b.	Is there any system connectivity with the entity which You are a subsidiary or franchisee of?			☐ Yes ☐ No
c.	Do You share any data with the entity which You are a subsidiary or franchisee of?			☐ Yes ☐ No
	If yes, please detail.			
d.	Does the entity which You are a subsidiary or franchisee hold insurance policies which You are entitled to claim under?			☐ Yes ☐ No
	If yes, please detail.			

1. Data Privacy

a.	For approximately how many unique individuals and organisations would You be required to notify in the event of a breach of Personally Identifiable Information (PII)?	
b.	Which of the following types of **Sensitive Records** do You store, process, transmit or otherwise have responsibility for securing?	
i.	Customers and business partners confidential information	☐ Yes ☐ No
ii.	Employee information	☐ Yes ☐ No
iii.	Personal Information (name, address)	☐ Yes ☐ No
iv.	TFN, Driving licence Passport or other ID	☐ Yes ☐ No
v.	Healthcare or medical records	☐ Yes ☐ No

vi.	Biometric information (If yes see appendix)	☐ Yes ☐ No
vii.	Credit card numbers, debit card numbers or other financial account numbers	☐ Yes ☐ No
	Other **Sensitive Records** - please specify	
c.	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

2. Information Security

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

b. 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 approval 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 and management
- ☐ Formal data classification policy
- ☐ Formal data retention plan
- ☐ 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 (IDS)**
- ☐ **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

1. Do You allow remote access to Your corporate network or operational technology environment? ☐ Yes ☐ No

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

   ☐ Remote Email ☐ Remote Access ☐ Internal Admin and **Privileged Accounts**

   ☐ **Remote Desktop Protocol (RDP)**

3. Please confirm the **Advanced 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

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

- ☐ Quarantine of suspicious email
- ☐ **Sandbox** detonation of attachment/links
- ☐ **Sender Policy Framework (SPF)**
- ☐ 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
- ☐ Restricted access via **MFA**
- ☐ Completely **Offline or Air-Gapped** (tape/non-mounted disks) backups that are disconnected from the rest of the network
- ☐ Immutable or **Write Once Read Many (WORM)** back up technology
- ☐ Fully Encrypted
- ☐ Other (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)
- ☐ Other (please describe):

3. Systems

a.	Do You use any end-of-life or unsupported hardware, software or systems?	☐ Yes ☐ No
b.	Do You use any **Operational Technology**? If yes, please see appendix.	☐ Yes ☐ No

c. **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**

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

Operational Technology (OT) Exposure Information

1.	Do You use any Operational Technology (OT)? *If yes, please provide the following information:*	☐ Yes ☐ No
a.	Do You have a formal OT security policy that includes cyber security?	☐ Yes ☐ No

b. Who is responsible for implementing and maintaining the cyber security of OT system and networks?

☐ IT Security organisation ☐ Engineering or business unit ☐ Other:

c. How many production sites are:

Operated by You	%	Operated by provider	%

d.	Are production sites segmented from one another to minimise the chance of multiple sites being impacted by the same event of incident?	☐ Yes ☐ No

e. How do You segregate OT from Information Technology assets and networks?

☐ VLAN ☐ Least privilege access controls ☐ Air-Gap

☐ Firewall configuration (access control list) ☐ Demilitarised zoning (DMZ) ☐ OT has restricted Internet access

☐ Data diode ☐ Host-based firewalls ☐ Other:

2.	Do you allow remote access to OT environments? *If yes, please complete the below:*	☐ Yes ☐ No

a. How is remote access to OT secured? *Select all that apply.*

☐ VPN (Virtual Private Network) ☐ **Multi-Factor Authentication (MFA)** ☐ SSO (Single Sign-on) via **MFA**

☐ **Zero Trust Network Access (ZTNA)** ☐ Traffic **Encryption** ☐ Other:

Please detail any exception to the above, or provide additional commentary:

3. Please describe Your patch management process and cadence for OT.

4.	Do You monitor and respond to events occurring in Your OT environment in the same way as Your Information Technology environment?	☐ Yes ☐ No
5.	Do You maintain and text backups of Your OT environment?	☐ Yes ☐ No

a. If Yes, how are these backups protected? *Select all that apply.*

☐ Immutable or **Write Once Read Many (WORM)** backup technology

☐ Completely **Offline or Air-gapped** (tape / non-mounted disks) backups

☐ Completely **Offline or Air-gapped** (tape / non-mounted disks) backups

☐ Restricted access to backups via **MFA**

☐ **Encryption** of backups

☐ OT backups are segmented from IT networks

☐ None of the above

☐ Other:

6. Please describe Your ability to rely on manual or other workaround procedures if systems are impacted by a cyber incident:

XIII. Loss History

1. Have You ever experienced any actual or potential **General Liability Claims**, **E&O/ PI Claims**, **Media Claims**, **Data Breaches**, or **Cyber Incidents** or allegations of performance failure in the past three years?	☐ Yes ☐ No

a. 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 **General Liability Claims**, **E&O/ PI Claims**, **Media Claims**, **Data Breaches**, or **Cyber Incidents**?	☐ Yes ☐ No

a. If Yes, please provide additional details:

Declaration

The undersigned authorised officer declares that to the best of their knowledge and belief the statements set forth herein and all attachments and schedules hereto are true and notice will be given as soon as reasonably practicable should any of the above information alter between the date of this proposal and the proposed date of inception of the insurance. Although the signing of the proposal does not bind the undersigned, on behalf of the Named Insured, to effect insurance, the undersigned agree that this proposal and all attachments and schedules hereto and the said statements herein shall be the basis of and will be incorporated in the policy should one be issued.

The undersigned, on behalf of the Named Insured and all of its subsidiaries, acknowledge that the Statutory Notice contained herein has been read and understood.

Name of Director, Officer, or Risk Manager:	
Signature:	
Date:	

Please enclose with this proposal form:

☐ A copy of your standard contract template

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

☐ Your most up-to-date financial statement

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. Other (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

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 PremierClimate, most common is arranging 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

Glossary of Defined Terms

Active Directory is a collection of objects within a Microsoft Active Directory network. An object can be a single user or a group, or it can be a hardware
component, such as a computer or printer. Each domain holds a database containing object identity information.

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/ PI 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 behaviors, use various data analytics techniques to detect suspicious system behavior, 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.

A **General Liability Claim** includes any claims for bodily injury, personal injury and property damage including product liability or product recall claims.

Heuristic Analysis - looks for suspicious properties in code, 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".

Intrusion Detection Systems (IDS) 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) 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 - as it 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 - 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.

Sender Policy Framework (SPF) is an email authentication method that is used to prevent unauthorised individuals from sending email messages from Your domain, and generally helps to protect email users and recipients from spam and other potentially dangerous emails.

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.

USA / Canada Domestic is turnover generated by Your company located inside the USA and Canada, for a customer that is also located in the USA or Canada.

USA / Canada Exports is defined as "Turnover generated by Your company located outside of the USA or Canada, for a customer located in the USA or Canada."

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

Zero Trust Network Access (ZTNA) is a service involving the creation of an identity and context-based, logical access boundary around an application or set of applications.

Duty of Disclosure

Your Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms.

You have this duty until we agree to insure you. You have the same duty before you renew, extend, vary or reinstate an insurance contract.

What you do not need to tell us

You do not need to tell us anything that:

- reduces the risk we insure you for; or
- is common knowledge; or
- we know or should know as an insurer; or
- we waive your duty to tell us about.

If you do not tell us something

If you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both.

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

Data Protection

Chubb Insurance Singapore Limited ("Chubb") is committed to protecting your personal data. Chubb collects, uses, discloses and retains your personal data in accordance with the Personal Data Protection Act 2012 and our own policies and procedures. Our Personal Data Protection Policy is available upon request.

Chubb collects your personal data (which may include health information) when you apply for, change or renew an insurance policy with us, or when we process a claim. We collect your personal data to assess your application for insurance, to provide you with competitive insurance products and services and administer them, and to handle any claim that may be made under a policy. If you do not provide us with your personal data, then we may not be able to provide you with insurance products or services or respond to a claim.

We may disclose the personal data we collect to third parties for and in connection with such purposes, including contractors and contracted service providers engaged by us to deliver our services or carry out certain business activities on our behalf (such as actuaries, loss adjusters, claims investigators, claims handlers, third party administrators, call centres and professional advisors, including doctors and other medical service providers), other companies within the Chubb Group, other insurers, our reinsurers, and government agencies (where we are required to by law). These third parties may be located outside of Singapore.

You consent to us using and disclosing your personal data as set out above. This consent remains valid until you alter or revoke it by providing written notice to Chubb's Data Protection Officer ("DPO") (contact details provided below). If you withdraw your consent, then we may not be able to provide you with insurance products or services or respond to a claim.

From time to time, we may use your personal data to send you offers or information regarding our products and services that may be of interest to you. If you do not wish to receive such information, please provide written notice to Chubb's DPO.

If you would like to obtain a copy of Chubb's Personal Data Protection Policy, access a copy of your personal data, correct or update your personal data, or have a complaint or want more information about how Chubb manages your personal data, please contact Chubb's DPO at:

Address: Chubb Data Protection Officer
138 Market Street
#11-01 CapitaGreen
Singapore 048946
E dpo.sg@chubb.com

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