CHUBB®

Cyber Enterprise Risk Management

Extensive Cyber Proposal Form

Important

Claims-Made and Claims-Made and Notified Coverages
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.

Notification of Facts that might give rise to a claim
Section 40(3) of the Insurance Contracts Act 1984 (Cth) ("ICA") only applies to the claims made and the claims made and notified coverages available under your policy.

Pursuant to Section 40(3) of the ICA, and only pursuant to that section, if you give notice in writing to us of facts that might give rise to a claim against you as soon as reasonably practicable after you become aware of such facts but before the insurance cover provided by your policy expires, then we are not relieved of liability under your policy in respect of the claim, when made, by reason only that it was made after the expiration of the period of the insurance cover provided by your policy.

Completing This Proposal Form

- Please read the "Duty of Disclosure" and "Privacy Statement" before completing this Proposal Form.
- **This Proposal Form is for Businesses with revenue of more than $700m.**
- It is agreed that whenever used in this Proposal Form, the term "You" and "Your" shall mean the Named Insured and all its Subsidiaries.
- Certain words appearing in green bold font have a certain meaning as per the glossary section below.
- This document allows Chubb to gather the needed information to assess the risks related to your information systems. If your information systems security policies differ between your companies or subsidiaries, please complete separate proposal forms for each information system.

I. Company Information

Company Name:		Website:	
Company headquarters (Address, City, Country, Postcode):		Year Established:	
		Number of Employees:	

Is your business a subsidiary, franchisee, or smaller entity of a larger organisation? □ Yes □ No

If Yes, please detail:

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):		Role:	
Email:		Phone:	

II. Company Profile

1. **Turnover** - Please describe how much turnover you generate

Turnover	Prior complete financial year	Estimated current year	Projected following year
Global	$	$	$

II. Company Profile *continued*

USA & Canada **Domestic**	**$**	**$**	**$**
USA & Canada **Exports**	**$**	**$**	**$**
Rest of World	**$**	**$**	**$**

Percentage of global turnover generated from online sales	%

Please detail the approximate percentage of your revenue applicable to each State, Territory and Overseas:

NSW	VIC	QLD	SA	WA	ACT	NT	TAS	O/S
%	%	%	%	%	%	%	%	%

2. **Business Activities** - Please describe what your company does to generate the turnover listed above, including subsidiary activities. Please include a % breakdown for each of the activities.

3. Do you provide ANY services to, or trade with individuals or organisations in sanctioned territories including but not limited to Iran, Syria, North Sudan, Crimea Region, North Korea, Venezuela, and Cuba, or any territory that is subject to certain US, EU, UN, and/or other national sanctions restrictions? □ Yes □ No

If Yes, please detail:

4. **Scope of Activities** - Do you have any company or subsidiary offices domiciled outside of your country of headquarters for which coverage is required? □ Yes □ No

a. If Yes, please complete the table below. If you need more space, please include as an attachment to this proposal.

Note: This information is to ensure that each of your entities are eligible for coverage in the countries in which you operate.

Name of subsidiary/entity	Country (if USA or Australia, please include the State)	% of global turnover generated

Additional commentary on business operations:

III. 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. Approximately how many unique individuals and organisations do you hold:

a) payment card information or financial account information	
b) health information records	

3. Do you process data on behalf of any third party? □ Yes □ No

a) If Yes, please describe:

4. Is any payment card information (PCI) processed in the course of your business? □ Yes □ No

a) If Yes, what is the estimated number of PCI transactions that you process annually?	

III. Data Privacy *continued*

4. b) Do you outsource your **PCI DSS** duties?	□ Yes □ No

c) Please describe your (or your outsourcer's) level of PCI DSS compliance:

□ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Not Compliant (please describe):

IV. Data and Information Security

1. Please indicate whether you have the following cyber and data governance, resourcing, and planning practices in place:

a) formal privacy policy approved by legal and management	□ Yes □ No
b) formal information security policy approved by legal and management	□ Yes □ No
c) formal data classification policy	□ Yes □ No
d) dedicated staff member(s) governing data security	□ Yes □ No
e) dedicated staff member(s) governing IT security	□ Yes □ No
f) formal cyber-specific incident response plan that is tested at least annually	□ Yes □ No
g) formal data breach response plan that is tested at least annually	□ Yes □ No
h) formal privacy law and regulation compliance monitoring	□ Yes □ No
i) cyber security is managed at the central/top level for all subsidiaries	□ Yes □ No
j) cyber security baseline is set at the central/top level for all subsidiaries to comply with	□ Yes □ No
k) locations and/or subsidiaries are audited for compliance with policies and baselines	□ Yes □ No

Additional commentary:

2. Please complete the following table as it applies to your privacy and security regulatory compliance:

Regulation or Directive	Compliance Assessed in the past 12 months?		Compliance Requirements Addressed?		Not Applicable
	Yes	*No*	*Yes*	*No*	
Australia - Notifiable Data Breach Scheme	□	□	□	□	□
UK - Data Protection Act	□	□	□	□	□
UK - NIS Directive	□	□	□	□	□
EU - GDPR	□	□	□	□	□
USA - HIPAA	□	□	□	□	□
USA - HITECH	□	□	□	□	□
USA - GBLA	□	□	□	□	□
California - CCPA / CPRA	□	□	□	□	□
Canada - PIPEDA	□	□	□	□	□

Other (please specify):

3. Please provide additional commentary on any non-compliance with relevant **Privacy Laws and Regulations** in applicable jurisdictions, along with plans in place to remediate:

II. Company Profile *continued*

USA & Canada **Domestic**	**$**	**$**	**$**
USA & Canada **Exports**	**$**	**$**	**$**
Rest of World	**$**	**$**	**$**

Percentage of global turnover generated from online sales	%

2. **Business Activities** - Please describe what your company does to generate the turnover listed above, including subsidiary activities. Please include a % breakdown for each of the activities.

3. Do you provide ANY services to, or trade with individuals or organisations in sanctioned territories including but not limited to Iran, Syria, North Sudan, Crimea Region, North Korea, Venezuela, and Cuba, or any territory that is subject to certain US, EU, UN, and/or other national sanctions restrictions?	□ Yes □ No

If Yes, please detail:

4. **Scope of Activities** - Do you have any company or subsidiary offices domiciled outside of your country of headquarters for which coverage is required? a. If Yes, please complete the table below. If you need more space, please include as an attachment to this proposal. *Note: This information is to ensure that each of your entities are eligible for coverage in the countries in which you operate.*	□ Yes □ No

Name of subsidiary/entity	Country (if USA or Australia, please include the State)	% of global turnover generated

Additional commentary on business operations:

III. 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. Approximately how many unique individuals and organisations do you hold:

a) payment card information or financial account information	
b) health information records	

3. Do you process data on behalf of any third party?	□ Yes □ No

a) If Yes, please describe:

4. Is any payment card information (PCI) processed in the course of your business?	□ Yes □ No
a) If Yes, what is the estimated number of PCI transactions that you process annually?	
b) Do you outsource your **PCI DSS** duties?	□ Yes □ No

c) Please describe your (or your outsourcer's) level of PCI DSS compliance:

□ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Not Compliant (please describe):	

IV. Data and Information Security

1. Please indicate whether you have the following cyber and data governance, resourcing, and planning practices in place:

a) formal privacy policy approved by legal and management	□ Yes □ No
b) formal information security policy approved by legal and management	□ Yes □ No
c) formal data classification policy	□ Yes □ No
d) dedicated staff member(s) governing data security	□ Yes □ No
e) dedicated staff member(s) governing IT security	□ Yes □ No
f) formal cyber-specific incident response plan that is tested at least annually	□ Yes □ No
g) formal data breach response plan that is tested at least annually	□ Yes □ No
h) formal privacy law and regulation compliance monitoring	□ Yes □ No
i) cyber security is managed at the central/top level for all subsidiaries	□ Yes □ No
j) cyber security baseline is set at the central/top level for all subsidiaries to comply with	□ Yes □ No
k) locations and/or subsidiaries are audited for compliance with policies and baselines	□ Yes □ No

Additional commentary:

2. Please complete the following table as it applies to your privacy and security regulatory compliance:

Regulation or Directive	Compliance Assessed in the past 12 months?		Compliance Requirements Addressed?		Not Applicable
	Yes	*No*	*Yes*	*No*	
Australia - Notifiable Data Breach Scheme	□	□	□	□	□
UK - Data Protection Act	□	□	□	□	□
UK - NIS Directive	□	□	□	□	□
EU - GDPR	□	□	□	□	□
USA - HIPAA	□	□	□	□	□
USA - HITECH	□	□	□	□	□
USA - GBLA	□	□	□	□	□
California - CCPA / CPRA	□	□	□	□	□
Canada - PIPEDA	□	□	□	□	□

Other (please specify):

3. Please provide additional commentary on any non-compliance with relevant **Privacy Laws and Regulations** in applicable jurisdictions, along with plans in place to remediate:

IV. Data and Information Security *continued*

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

5. Please complete the following as it relates to biometric information:

a) Do you and others on your behalf or at your direction collect, store or transmit biometric information, including but not limited to fingerprints, retina scans, or time clocks that rely on individual identifiers?	□ Yes □ No

If Yes, please complete the "Biometric Information" supplemental questions at the end of this document.

6. Please complete the following questions as it relates to **Personally Identifiable Information (PII)** storage and protection:

a) What percentage of **PII** is encrypted at rest at the field/specific data level?	%
b) What percentage of **PII** is encrypted at rest at the field level?	%
c) Is **PII** encrypted in transit?	□ Yes □ No
d) Do you segment **PII** by the following to minimise the potential impact of a **Data Breach**:	
i) Business Segment	□ Yes □ No
ii) Contract or customer	□ Yes □ No
iii) Geography	□ Yes □ No
iv) Other (please specify):	
e) Have you implemented **Enterprise or Integrated Data Loss Prevention (DLP)** tools?	□ Yes □ No

i) If Yes, how is this configured?

□ Blocking mode □ Alert mode only □ Manual intervention required □ Automation implemented □ Anomaly detection enabled

f) If **PII** is segmented, please indicate the total number of unique individuals that would exist in a single database or repository	
7. Do you utilise any **Microsegmentation** for databases with more highly regulated or sensitive **PII**?	□ Yes □ No
8. Is access to databases with **PII** limited to a need-to-know basis?	□ Yes □ No

9. Do you actively enforce any of the following to minimise sensitive personal data exposures:

□ Data anonymisation □ Data pseudonymisation □ Data tokenisation □ Other similar techniques:

Please comment on how widely this is implemented throughout your business:

10. Do you outsource the processing of **PII** to data processor(s)?	□ Yes □ No
a) Do you maintain written contracts with such providers at all times?	□ Yes □ No
b) Have these contracts been reviewed for compliance with privacy regulations?	□ Yes □ No
c) Do these contracts address which party is responsible for responding to a **Data Breach**?	□ Yes □ No

Additional commentary on **PII** storage and collection:

V. Technical Controls and Processes

Network structure and access

1. Are critical systems and applications hosted centrally?	□ Yes □ No □ Partial
2. Do you operate on a “flat” network?	□ Yes □ No

3. Please detail how your network has been structured or segmented in order to minimise lateral movement of malware or users within your organisation:

Does this utilise:

□ VLAN	□ Software Defined Networking (SDN)
□ Air-gap	□ Lease privilege access controls
□ Host-based firewalls	□ Other:
□ Firewall configuration (access control list)	

4. Please detail how applications and systems are segregated to minimise the chance of multiple services being impacted by an issue or vulnerability in a specific application or system:

Does this utilise:

□ VLAN	□ Software Defined Networking (SDN)
□ Air-gap	□ Least privilege access controls
□ Host-based firewalls	□ Other:
□ Firewall configuration (access control list)	

5. Do you conduct penetration testing at least annually to assess the security of important externally facing systems?	□ Yes □ No
6. Do you conduct penetration testing on important internal systems at least annually?	□ Yes □ No
7. Do you have a **Web Application Firewall (WAF)** in front of critical externally facing applications?	□ Yes □ No
8. Do you allow mobile devices (including laptops, tablets, and smartphones) to access company or network applications and resources?	□ Yes □ No

a) What percentage of mobile devices are **Managed Devices**, or you have enabled and enforced a **Mobile Device Management** product?

1. Company issued laptops	%	□ N/A
2. Company issued tablet computers	%	□ N/A
3. Company-issued smartphones	%	□ N/A
4. Bring Your Own Device (BYOD) *(including laptops, tablets, and smartphones)*	%	□ N/A

9. Does any part of your corporate network maintain remote access capability?	□ Yes □ No

If Yes, please complete the below:

a) How is remote access to your corporate network secured? *(select all that apply)*

□ VPN (Virtual Private Network)	□ ZTNA (Zero Trust Network Access)
□ SSO (Single Sign-on) via **MFA**	□ Other:
□ Traffic **Encryption**	
□ **Multi-Factor Authentication**	

V. Technical Controls and Processes *continued*

10. Please detail your use of **Remote Desktop Protocol (RDP)**:

□ RDP is not used at all

□ RDP is used for remote access

□ RDP is limited to internal use only

□ RDP is used in another capacity:	

a) If RDP is used in any capacity, which of the following are implemented? *(select all that apply)*

□ VPN (Virtual Private Network)	□ Multi-Factor Authentication
□ NLA (Network Level Authentication)	□ RDP honeypots established
□ Other:	

Directory, Domains, and Accounts

11. Do you have a formal **Identity and Access Management** programme in place?	□ Yes □ No
12. How many privileged users have full access to your directory service, including your **Active Directory Domain**?	
13. How many users have persistent administrative access to workstations and servers other than their own?	
14. How many total number of users have administrative access?	

15. Please detail why this number of **Privileged Accounts** is necessary:

16. Please detail how accounts are managed:

□ Local, domain, and service accounts are manually reviewed to check for unauthorised creation of new accounts

• If applicable, indicate frequency of review:	

□ Directory service (including **Active Directory Domain**) is monitored in real time to detect unusual activity

□ A third party tool is used to audit, session monitor, and administer service accounts

□ Service accounts are not assigned to privileged groups, such as local or domain admin groups

17. Have you disabled all local administrative accounts?	□ Yes □ No

a) If No, please provide details on how this is managed:

V. Technical Controls and Processes *continued*

18. Do you require that network administrators have separate accounts for 'regular' and 'privileged' access with separate login, password, and authentication?	□ Yes □ No
19. Do you utilise **Privileged Access Workstations** that have no access to email or internet?	□ Yes □ No
20. Are access logs stored for at least 90 days?	□ Yes □ No
21. Have you segregated administrator access according to **Microsoft's Active Directory Administrative Tier Model** (or similar)?	□ Yes □ No □ N/A
22. Is the use of **Privileged Accounts** monitored and automatically logged off when not in use?	□ Yes □ No
23. Is the use of **Privileged Accounts** controlled by a **Privileged Access Management (PAM)** solution?	□ Yes □ No
24. Does privileged access require separate **Multi-Factor Authentication** for internal or on-network access?	□ Yes □ No
25. How many emergency **Privileged Accounts** do you maintain that do not require **MFA**?	
a) Are emergency accounts required to maintain a password of at least 30 characters?	□ Yes □ No □ N/A

b) How do you securely store and protect the password to these accounts?

Comments applicable to access controls, directory services (including **Active Directory Domain**), and **Privileged Accounts**:

Authentication

26. Where you have implemented **Multi-Factor Authentication**, has this solution been configured in a way where the compromise of any single device will only compromise a single authentication factor?	□ Yes □ No □ N/A

Additional commentary:

Email Security

27. Do you require **Multi-Factor Authentication** for webmail or cloud-hosted email access?	□ Yes □ No □ N/A

28. Please detail how your email activity is secured *(select all that apply)*:

□ Applicable emails are tagged or labelled as "External" or similar

□ Sender Policy Framework (SPF) is enforced on all incoming emails

□ Domain Keys Identified Mail (DKIM) is enforced

□ All incoming email goes through a secure email gateway

□ All incoming email is scanned and filtered for malware

□ All suspicious emails are automatically placed into quarantine

□ Sandboxing is used for further investigation of email attachments

□ External emails that are deemed to be sensitive are securely sent

□ All employees are trained on the risks of phishing and other social engineering threats

□ Microsoft Office macros are disabled from running by default

□ None of the above

□ Other:

Additional commentary on email security:

V. Technical Controls and Processes *continued*

Business Continuity and Disaster Recovery

29. Do you have a formal Business Continuity Plan that addresses cyber scenarios? □ Yes □ No

a) Is this tested at least annually? □ Yes □ No □ N/A

30. Do you have a formal Disaster Recovery Plan that addresses cyber scenarios? □ Yes □ No

a) Is this tested at least annually? □ Yes □ No □ N/A

31. Please generally describe your backup procedures for data(bases) and systems:

32. Please provide some additional details on ransomware-safe backup strategies related to disaster recovery:

a) How are backups protected? *(select all that apply)*:

- □ Immutable or **Write Once Read Many (WORM)** backup technology
- □ Completely **Offline / Air-gapped** (tape / non-mounted disks) backups disconnected from the rest of your network
- □ Restricted access via separate **Privileged Account** that is not connected to **Active Directory** or other domains
- □ Restricted access to backups via **MFA**
- □ **Encryption** of backups
- □ Cloud-hosted backups segmented from your network
- □ None of the above
- □ Other:

33. Are full restore from backup tests performed at least annually? □ Yes □ No

34. Do you test for recoverability as well as integrity? □ Yes □ No

35. Does your backup and restore plan include specific ransomware scenarios? □ Yes □ No

36. Do you scan data and information for malware or viruses prior to backup □ Yes □ No

37. Do you have specific backup procedures for email records? □ Yes □ No

38. Please describe the information systems, applications, or services (both internally and externally hosted) on which you depend most to operate your business:

Regarding outsourced services, this may include cloud services, data hosting, business application services, co-location, data back-up, data storage, data processing, or any similar type of outsourced computing or information services.

Name of System, Application, or Service	Provider Name (if outsourced) If internal put "N/A"	Has a Business Impact Analysis been performed?	Do you have a defined **Recovery Point Objective**?	**Recovery Time Objective** (hours)	Please detail your backup frequency

V. Technical Controls and Processes *continued*

39. Do you maintain alternative systems for critical applications? □ Yes □ No

a) If Yes, please select from the following:

□ Automatic failover (Active - Active)

□ Automatic failover (Active - Passive)

□ Manual failover

□ Colocation facility

□ Offline alternative environment

□ Alternative provider (if outsourced)

□ Other (please describe):

40. Do you have alternate power for mission critical or revenue generating equipment? □ Yes □ No

41. Do you have the ability to procure extra bandwidth from alternative suppliers? □ Yes □ No

42. Do you use and test backup power generators, dual supply units, or other equipment to offset power outage or failure as part of business continuity or disaster recovery plans? □ Yes □ No

43. Do your software developers receive training on the principles of writing secure applications? □ Yes □ No

44. Please describe quality control and testing procedures that apply to any new software programmes (including updates and new releases to existing software) on your network (including minimal timeframe for a new or updated system to pass quality assurance testing before it is made operational on your live network, along with separate development, testing, and acceptance environments)

Prevention, Monitoring, and Incident Response

45. Do you have plans and protections in place for Distributed Denial of Service (DDoS) attacks? □ Yes □ No

46. Do you utilise any **Threat Intelligence** sources or services? □ Yes □ No

47. How do you prevent, monitor and respond to cyber incidents and alerts? *(select all that apply)*

□ **Intrusion Detection System**

□ Intrusion Prevention System

□ Advanced or next-generation anti-malware and anti-virus with **Heuristic Analysis**

□ **URL filtering or Web Filtering**

□ **Application Isolation & Containment**

□ **Advanced Endpoint Protection**

□ **Endpoint Detection and Response (EDR)**

□ **Managed Detection and Response (MDR)**

□ **Extended Detection and Response (XDR)**

- Please provide percentage of endpoints covered by EDR, MDR, or XDR above: %
- Provider of EDR, MDR, or XDR tools:
- Is this tool configured to automatically isolate or block activity? □ Yes □ No
- Are alerts from EDR, MDR, or XDR tools fed into a **Security Information and Event Monitoring (SIEM)**, **Security Orchestration, Automation, and Response (SOAR)**, or **Centralised Endpoint Protection Platform** (or similar) system? □ Yes □ No

V. Technical Controls and Processes *continued*

□ Manual Log reviews	
□ **Security Information and Event Monitoring (SIEM)** tool	
• Please provide percentage of critical log information that feeds into SIEM	%
• SIEM tool provider:	
□ **Security Operations Centre (SOC)** in place	
□ Internal	
□ External	
□ Hybrid	
□ 24/7 operations	
□ **Security Orchestration, Automation, and Response (SOAR)** solution	
□ Managed firewall service	
□ **Protective Domain Name System (DNS)** service	
□ Other monitoring tools or services (please detail):	

Asset and Configuration Management

48. Do you maintain an inventory of all hardware and software assets?	□ Yes □ No
a) What percentage of your assets is included in this inventory?	%
b) What percentage of your assets are within scope for vulnerability scanning?	%
49. Do you utilise any **Configuration Management Databases (CMDB)**?	□ Yes □ No □ Partial
50. Do you assign risk levels each asset in your inventory to prioritise patching and vulnerability management actions?	□ Yes □ No
51. How often do you perform internal vulnerability scans?	
52. How often do you perform external vulnerability scans?	
53. Which vulnerability management tools do you utilise?	
a) External scanning:	
b) Internal scanning:	
□ Not applicable	
54. Please outline your use of end-of-life or unsupported hardware, software, or systems:	
a) Are any of these processes, systems, or applications business-critical?	□ Yes □ No
b) Do you store or process and sensitive personal or corporate confidential information on these systems?	□ Yes □ No
c) Are these systems restricted from internet access?	□ Yes □ No
d) Are these systems segregated and isolated from other parts of your network?	□ Yes □ No
e) Please outline which end-of-life or unsupported systems you operate, what they are used for, and how many are used in your business:	

V. Technical Controls and Processes *continued*

f) Please outline your decommissioning plans and timelines:

g) Please outline other mitigating controls in place to minimise lateral movement from unsupported systems to other environments within your network:

55. Do you regularly scan your external firewalls for any unnecessary open ports?	□ Yes □ No
56. Do you disable all non-essential open ports and protocols?	□ Yes □ No
57. Do you have a formal patch management process in place?	□ Yes □ No

58. Target timelines depending on vulnerability criticality (**Common Vulnerability Scoring System – CVSS**)

• Low		days
• Medium		days
• High		days
• Critical		days

59. Please detail your level of compliance with these targets over the most recent 12 months:

60. If a patch can not be applied in a timely manner, what actions do you take to mitigate vulnerability risk?

61. Are patches tested in a controlled environment before deploying more broadly?	□ Yes □ No

Additional commentary:

VI. Third Party Risk Management

For this section, third party technology providers may include cloud services, data hosting, business application services, co-location, data back-up, data storage, data processing, or any similar type of outsourced computing or information services.

1. Do you have dedicated vendor management resources?	□ Yes □ No
2. Do you perform assessments or audits to ensure third party technology providers meet your company's data and information security requirements?	□ Yes □ No □ Partial
3. Do you perform risk-based assessments on which technology vendors are most critical to your business?	□ Yes □ No □ Partial

4. Please indicate who is involved in choosing and assessing technology vendors, suppliers, and service providers:

□ Vendor management resource

□ Risk management resource

□ Legal resource

□ Business unit resource

□ Technical information technology resource

□ Other:

VI. Third Party Risk Management *continued*

5. Please indicate applicable contingency planning for business-critical outsourced technology services:

□ Alternative service providers are available for use in case of primary provider unavailability

□ Contracts are in place with some alternative providers

□ Alternative providers have been identified, but not contracted with

□ Single-source providers are used for most business-critical outsourced technology services

Additional commentary on your management of and reliance on outsourced technology providers:

6. Please select what is included in vendor assessments, either prior to contracting or during audits:

□ Information security certification review

□ Business resilience certification review

□ Penetration testing

□ Cyber security rating service (BitSight, SecurityScorecard, OneTrust, Prevalent, or similar)

□ Review of vendor's backup procedures

□ Service Level Agreement (SLA) assessment

□ **Multi-Factor Authentication** review

□ Data Protection Impact Assessment performed

□ Data Protection Agreements included in contracts

□ Other:

7. How often do you waive your right of recourse against any third party technology providers in the event of service disruption?

□ Never or infrequently

□ Sometimes

□ Always or most of the time

□ Other commentary:

Cloud Security

8. Do you utilise cloud applications, platforms, infrastructure, or other services?	□ Yes □ No
9. Do you have a formal cloud security policy?	□ Yes □ No □ N/A

10. Please indicate which of the following you have implemented to support cloud security initiatives:

□ **Cloud Access Security Broker (CASB)**

□ Secure Access Service Edge (SASE) model enforced

□ Zero Trust Network Access (ZTNA) cloud model enforced

□ Single Sign On (SSO) used for authentication to cloud services

□ **Multi-Factor Authentication** required to access business critical cloud applications

□ **Multi-Factor Authentication** required to access non-business critical cloud applications

11. Please detail any exceptions to the **MFA** responses above, or provide additional commentary:

VI. Third Party Risk Management *continued*

Acquisitions

12. How many acquisitions have you made over the past three years?	

13. Please detail name of entities acquired, size of entities, and dates of acquisitions:

14. When do you audit and assess the cyber security posture and exposure of such entities?

□ Before acquisition

□ After acquisition but before integration

□ Assessments of cyber security are rarely performed before or after acquisition

□ Other:

15. Please detail integration strategy, timelines, and due diligence performed regarding acquired entities:

VII. Media

1. Has legal counsel screened the use of all trademarks and service marks, including your use of domain names and metatags, to ensure they do not infringe on the intellectual property rights of others?	□ Yes □ No
2. Do you obtain written permissions or releases from third party content providers and contributors, including freelancers, independent contractors, and other talent?	□ Yes □ No
3. Do you involve legal counsel in reviewing content prior to publication or in evaluating whether the content should be removed following a complaint?	□ Yes □ No
4. Do you contract with third parties providers, including outside advertising or marketing agencies, to create or manage content on your behalf?	□ Yes □ No
a) If Yes, do you require indemnification or hold harmless agreements in your favour?	□ Yes □ No
5. Has your privacy policy, terms of use, terms of service and other customer policies been reviewed by counsel?	□ Yes □ No

VIII. Loss History

1. Please indicate which of the following you have experienced in the past five years (please do not indicate events that have been mitigated by existing security measures):

□ **Data Breach**

□ Malicious **Cyber Incident** against you

□ **System Failure Event**

□ **Media Claim**

□ Regulatory Actions related to data or system security

□ **Data Breach** at a third party provider of yours

□ **Cyber Incident** impacting a third party provider of yours

a) If Yes to any of the above, please provide:

Description of any claims/incidents and date of occurrence:

VIII. Loss History *continued*

Description of the financial impact to your business:

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

2. Are you aware of any notices, facts, circumstances, or situations that could qualify as a **Data Breach, Cyber Incident, System Failure Event** or reasonably give rise to any **Media Claim** or Cyber or Data related Regulatory Actions?	□ Yes □ No

a) If Yes, please provide additional details:

Supplemental Questions - only complete these sections if applicable to your business

IX. 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):	

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:

X. Operational Technology

For this section, operational technology (OT) differs from information technology (IT) in that OT is focused on monitoring, managing, and controlling industrial operations or physical equipment, while IT is focused on electronic data exchange, processing, and storage. 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.

1. Do you have a formal OT security policy that includes cyber security?	□ Yes □ No

2. Who is responsible for implementing and maintaining the cyber security of OT systems and networks?

□ IT security organisation

□ Engineering or business unit

□ Other:

X. Operational Technology *continued*

3. How many production sites do you operate?				
a) What percentage are:	• operated by you	%	• operated by a provider	%
4. On average, what percentage of maximum capacity are production facilities running at?				%
5. Are production sites segmented from one another to minimise the chance of multiple sites being impacted by the same event or incident?				□ Yes □ No
6. Are your OT environments segmented from the Internet?				□ Yes □ No

7. How do you segregate OT from Information Technology?

□ VLAN

□ Air-gap

□ Host-based firewalls

□ Firewall configuration (access control list)

□ Demilitarised zoning (DMZ)

□ Data diode

□ Least privilege access controls

□ None of the above

□ Other:

8. Do you allow remote access to OT environments?	□ Yes □ No

If Yes, please complete the below:

a) How is remote access to OT secured? *(select all that apply)*

□ VPN (Virtual Private Network)	□ **Multi-Factor Authentication**	
□ SSO (Single Sign-on) via **MFA**	□ **Zero Trust Network Access (ZTNA)**	
□ Traffic **Encryption**	□ Other:	

- What percentage of users are these requirements applicable to?

1. Standard employees	%	or	□ N/A
2. Contractors	%	or	□ N/A
3. Vendors/suppliers	%	or	□ N/A
4. Privileged users	%	or	□ N/A

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

9. Please describe your patch management process and cadence for OT

10. For OT devices with critical vulnerabilities that cannot be patched or updated, please describe other compensating controls that you have in place to prevent exploitation of these devices:

X. Operational Technology *continued*

11. Do you monitor and respond to events occurring in your OT environment in the same way as your Information Technology environment?	□ Yes □ No
12. Do you maintain and test 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 / Air-gapped** (tape / non-mounted disks) backups

□ Restricted access via separate **Privileged Account** that is not connected to **Active Directory** or other domains

□ Restricted access to backups via **MFA**

□ **Encryption** of backups

□ OT backups are segmented from IT networks

□ None of the above

□ Other:

13. Are you able to make up for any lost production by increasing production at other sites or facilities, in the case of network or system outages?	□ Yes □ No
14. On average, how many days of stock or finished inventory do you maintain at production facilities or distribution locations that could continue to be sold even if production is halted?	days

15. Please describe your ability to rely on manual or other workaround procedures if systems are impacted by cyber incident

XI. Professional Services

1. Do you purchase any professional indemnity insurance?	□ Yes □ No
2. If yes, does your policy contains any applicable cyber exclusions?	□ Yes □ No
3. Do you operate, manage, or host any technology systems in support of your professional services?	□ Yes □ No
a) Are data and systems related to such services the responsibility of your customer?	□ Yes □ No

Please detail:

b) If you do host data and systems for your customers, do controls described in this proposal form apply to these hosted systems as it relates to resiliency, backup strategies, and data privacy compliance?	□ Yes □ No

Additional commentary:

XII. Retail Operations

1. Do you segregate your Point of Sale or transaction processing equipment and networks from other IT networks?	□ Yes □ No

2. Please describe your patch management process and cadence for Point of Sale software applications:

XII. Retail Operations *continued*

1. Do you segregate your Point of Sale or transaction processing equipment and networks from other IT networks? □ Yes □ No

2. Please describe your patch management process and cadence for Point of Sale software applications:

3. What percentage of your Point of Sale and/or payment terminals support chip technology meets EMV standards? %

4. Please name the provider(s) do you rely on for payment processing:

5. Are Point of Sale systems protected by antimalware and monitored by your information security resources? □ Yes □ No

   Additional commentary:

6. Do you have any franchisee locations or agreements? □ Yes □ No

   a) If Yes, please provide more information on who is responsible for cyber security at franchisees, and how cyber security controls are consistently applied:

XIII. Cyber Improvements *(optional)*

1. Please outline what improvements you have planned for the next ~12 months as it relates to cyber or information security and management:

XIV. Declaration

The undersigned authorised officers of the named Insured declare that to the best of their knowledge and belief the statements made in this proposal and in all attachments and schedules to this proposal are true and are true and notice will be given as soon as practicable should any of the above information change 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 to this proposal and the said statements in this proposal 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 in this proposal has been read and understood.

Name of Director, Officer or Risk Manager:

Signature:

Date:

Glossary of Defined Terms

Active Directory Domain - 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.

Application Isolation & Containment - this technology can block, restrict, or isolate specific endpoints from performing potentially harmful actions between endpoints and other applications or resources with the goal to limit the impact of a compromised system or endpoint.

Centralised Endpoint Protection Platform - is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Cloud Access Security Broker (CASB) - is software that monitors the activity between cloud service users and cloud applications to enforce security policies and prevent malicious activity.

Common Vulnerability Scoring System (CVSS) - is an open industry standard assessment of the severity of vulnerabilities, assigning scores depending on ease and potential impact of exploits.

Configuration Management Databases (CMDB) - is a database used to store information on hardware and software assets of an organisation, and is typically used to identify and manage the configuration of and the relationship between assets.

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 - means an incident where sensitive personal or corporate confidential information has been taken, lost, or viewed by an unauthorised party.

Domain Keys Identified Mail (DKIM) - is a standard email authentication method that adds a digital signature to outgoing messages to allow for improved verification of sender.

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

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.

Enterprise or Integrated Data Loss Prevention (DLP) - are software products and rules focused on preventing loss, unauthorised access, or misuse of sensitive or critical information. Enterprise DLP describes dedicated solutions implemented across an organisation and may include alerts, encryption, monitoring, and other movement control and prevention for data at rest and in motion. Integrated DLP utilises existing security tool services and add-ons to accomplish the same goal of preventing data loss and misuse.

Exports - is turnover generated by your company located outside of the USA or Canada, for a customer located in the USA or Canada.

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 - going beyond traditional signature-based detection in basic antivirus software, 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”.

Identity and Access Management (IAM) - ensures that the right users have the appropriate access to technology resources, and includes the management of usernames, passwords, and access privileges to systems and information

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.

Managed Device - is a device that requires a managing agent or software tool that allows information technology teams to control, monitor, and secure such device. A non-managed device would be any device that can not be seen or managed by such products or technology teams.

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

Microsegmentation - is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.

Microsoft's Active Directory Administrative Tier Model - is designed to reduce the risk of privilege escalation within a Microsoft Active Directory. In this model, assets are segregated into access privilege groups.

- Tier 0 - includes assets that provide direct control of security and identity - including the Active Directory and other identity and access management systems.
- Tier 1 - typically includes servers, applications, and cloud services that support critical business data and services.
- Tier 2 - Typically includes common workstations and user devices

Mobile Device Management (MDM) - is software that is installed on a managed device that allows information technology administrators to control, monitor, and secure mobile device endpoints.

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.

PCI DSS - 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.

Personally Identifiable Information (PII) - means any data that can be used to identify a specific individual. This may include health or medical records of employees or customers, government issued identification numbers, login usernames, email addresses, credit card numbers, biometric information, and other related personal 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 Access Workstations - is a hardened workstation configured with security controls and policies that restrict local administrative access and productivity tools to minimise the attack surface to only what is absolutely required for performing sensitive job tasks. These workstations typically have no access to email or general web browsing.

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

Protective Domain Name System - is a service which prevents access to domains known to be malicious, and also allows for additional analysis and alerts regarding blocked domain requests.

Recovery Point Objective (RPO) - is the maximum acceptable amount of time that may pass after an unplanned outage or incident before the quantity of data lost during that time exceeds the tolerance set in a Business Continuity Plan.

Recovery Time Objective (RTO) - means the targeted duration of time within which a business process must be restored after an outage or disruption in order to avoid unacceptable consequences associated with a break in business continuity.

Remote Desktop Protocol (RDP) - is a Microsoft protocol that allows for remote use of a desktop computer. Without additional protections, RDP has some serous security vulnerabilities.

Sandboxing - as it 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.

Secure Access Service Edge (SASE) - is a cloud-delivered service that combines cloud based network and security functions such as SWG, CASB, ZTNA with WAN capabilities.

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.

Security Operations Centre (SOC) - is a centralised function involving people, processes, and technology designed to continuously monitor, detect, prevent, analyse, and respond to cyber security incidents.

Security Orchestration, Automation, and Response (SOAR) - is technology used to automatically streamline and prioritise cyber security alerts from a collection of sources, including endpoints and applications (similar to a Security Information and Event Monitoring solution) but offers enhanced automated response and improved prediction techniques.

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.

Single Sign On (SSO) - is a method of authentication that enables users to authenticate securely with multiple applications and websites without logging into each one individually. This involves a trust relationship set up between an application, known as the service provider, and an identity provider.

System Failure Event - is the unintended breakdown, outage, disruption, inaccessibility to, or malfunction of computer systems or software caused by non-malicious means. A system failure event may be caused by a power failure, human error, or other disruption.

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.

Web Application Firewall (WAF) - is a type of network, host, or cloud-based firewall placed between an application and the Internet to protect against malicious traffic, and other common web attacks that typically target sensitive application data.

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.

Statutory Notice

For the purposes of this statutory notice, Chubb Insurance Australia Limited ABN: 23 001 642 020 AFSL: 239687 means “we”, “us” and “our”.

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.

Other Important Information

Subrogation

You may prejudice your rights with regard to a claim if, without prior agreement from us (such agreement not to be unreasonably withheld or delayed), you make agreement with a third party that will prevent us from recovering the loss from that, or another party.

Your policy contains provisions that either exclude us from liability, or reduce our liability, if you have entered into any agreements that exclude your rights to recover damages from another party in relation to any loss, damage or destruction which would allow you to sustain a claim under your policy.

Utmost Good Faith

Every insurance contract is subject to the doctrine of utmost good faith which requires that all parties to the contract, including third parties, should act toward each other with the utmost good faith. Failure to do so on your part may prejudice any claim or the continuation of cover provided by us. Our failure to do so could result in a civil penalty.

Not a Renewable Contract

Cover under your policy will terminate at expiry of the period of insurance specified in your policy document. If you wish to effect similar insurance for a subsequent period, it will be necessary for you to complete a new proposal form prior to the termination of your current policy so that terms of insurance and quotation/s can be agreed.

Change of Risk or Circumstances

It is vital that you advise us as soon as reasonably practicable of any departure from your “normal” form of business (i.e. that which has already been conveyed to us).

For example, acquisitions, changes in location or new overseas activities. Please refer to the territory clause of your policy and the sanctions limitations contained within your policy. You can contact us using the below details under ‘Contact Us’.

General Insurance Code of Practice

We are a signatory to the General Insurance Code of Practice (Code). The objectives of the Code are to further raise standards of service and promote consumer confidence in the general insurance industry. Further information about the Code and your rights under it is available at codeofpractice.com.au and on request. As a signatory to the Code, we are bound to comply with its terms. As part of our obligations under Parts 9 and 10 of the Code, Chubb has a Customers Experiencing Vulnerability & Family Violence Policy (Part 9) and a Financial Hardship Policy (Part 10). The Code is monitored and enforced by the Code Governance Committee.

Privacy Statement

In this Statement, **We**, **Our** and **Us** means Chubb Insurance Australia Limited (**Chubb**).

You and **Your** refers to Our customers and prospective customers as well as those who use Our Website.

This Statement is a summary of Our Privacy Policy and provides an overview of how We collect, disclose and handle Your Personal Information. Our Privacy Policy may change from time-to-time and where this occurs, the updated Privacy Policy will be posted to Our website.

Chubb is committed to protecting Your privacy. Chubb collects, uses and retains Your Personal Information in accordance with the requirement of the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (**APPs**), as amended or replaced from time-to-time.

Why We collect Your Personal Information

The primary purpose for Our collection and use of Your Personal Information is to enable Us to provide insurance services to You.

Sometimes, We may use Your Personal Information for Our marketing campaigns and research, in relation to new products, services or information that may be of interest to You.

How We obtain Your Personal Information

We collect Your Personal Information (which may include sensitive information) at various points including, but not limited to, when You are applying for, changing or renewing an insurance policy with Us or when We are processing a claim. Personal Information is usually obtained directly from You, but sometimes via a third party such an insurance intermediary or Your employer (e.g., in the case of a group insurance policy). Please refer to Our Privacy Policy for further details.

When information is provided to Us via a third party We use that information on the basis that You have consented or would reasonably expect Us to collect Your Personal Information in this way. We take reasonable steps to ensure that You have been made aware of how We handle Your Personal Information.

When do We disclose Your Personal Information?

We may disclose the information We collect to third parties, including:

- the policyholder (where the insured person is not the policyholder, i.e. group policies);
- service providers engaged by Us to carry out certain business activities on Our behalf (such as claims assessors, call centres in Australia, online marketing agency, etc);
- intermediaries and service providers engaged by You (such as current or previous brokers, travel agencies and airlines);
- government agencies (where we are required to by law);
- other entities within the Chubb group of companies such as the regional head offices of Chubb located in Singapore, UK or USA (Chubb Group of Companies); and
- third parties with whom We (or the Chubb Group of Companies) have sub-contracted to provide a specific service for Us, which may be located outside of Australia (such as in the Philippines or USA). These entities and their locations may change from time-to-time. Please contact us, if you would like a full list of the countries in which these third parties are located.

In the circumstances where We disclose Your Personal Information to the Chubb Group of Companies, third parties or third parties outside Australia We take steps to protect Personal Information against unauthorised disclosure, misuse or loss.

Your decision to provide Your Personal Information

In dealing with Us, You agree to provide Us with Your Personal Information, which will be stored, used and disclosed by Us as set out in this Privacy Statement and Our Privacy Policy.

Access to and correction of Your Personal Information

Please contact Our customer relations team on 1800 815 675 or email CustomerService.AUNZ@chubb.com if you would like:

- a copy of Our Privacy Policy, or
- to cease to receive marketing offers from Us or persons with whom We have an association.

To request access to, update or correct Your Personal Information held by Chubb, please complete this Personal Information request form and return it to:

Email: CustomerService.AUNZ@chubb.com
Fax: + 61 2 9335 3467
Address: GPO Box 4907, Sydney NSW 2001

Further information request
If You would like more information about how We manage Your Personal Information, please review Our Privacy Policy for more details, or contact:

Privacy Officer
Chubb Insurance Australia Limited
GPO Box 4907
Sydney NSW 2001
+61 2 9335 3200
Privacy.AU@chubb.com

How to make a complaint
If You are not satisfied with our organisation, services, Our response to Your enquiry, or You have any concerns about Our treatment of Your Personal Information or You believe there has been a breach of Our Privacy Policy, or You are not satisfied with any aspect of your relationship with Chubb and wish to make a complaint, please contact our Complaints and Customer Resolution Service (**CCR Service**) by post, phone, fax, or email, (as below):

Complaints and Customer Resolution Service
Chubb Insurance Australia Limited
GPO Box 4065
Sydney NSW 2001
P +61 2 9335 3200
F +61 2 9335 3411
E complaints.AU@chubb.com

For more information, please read Our Complaints and Customer Resolution policy.

About Chubb in Australia

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for 100 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages including Business Package, Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, to a broad client base, including many of the country's largest companies. Chubb also serves successful individuals with substantial assets to insure and consumers purchasing travel insurance.

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

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
www.chubb.com/au

Chubb. Insured.℠